DIPLOMARBEIT

Migration einer NT 4.0 Domäne in eine Windows 2003 Domäne

Ausgeführt zum Zweck der Erlangung des akademischen Grades eines

Dipl.-Ing. (FH) für Telekommunikation und Medien

am Fachhochschul-Diplomstudiengang

Telekommunikation und Medien St. Pölten

unter der Erstbetreuung von

Dipl.-Ing. Johann Mühlehner

Zweitbegutachtung von

Ing. Karl Lienbacher

ausgeführt von

Markus Gatty

Personenkennzahl: 0210038035

Amstetten, im September 2006 Unterschrift: _____

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

Diese Arbeit stimmt mit der vom Begutachter beurteilten Arbeit überein.

....

Ort, Datum Unterschrift

Kurzfassung

Auch wenn das Betriebssystem Microsoft Windows NT 4.0 bereits in die Jahre gekommen ist und mittlerweile als veraltetes Betriebssystem angesehen wird, existieren noch immer Umgebungen, welchen eine Migration bevorsteht. Je nach Größe der vorhandenen Domäne, stellt eine Umstellung auf ein neues System für die verantwortlichen Administratoren eine wesentliche Herausforderung dar. In dieser Arbeit soll daher ein Verständnis für die Anforderungen und Auswirkungen einer Migration entwickelt werden und darauf aufbauend ein Leitfaden von der Planung bis hin zur Implementierung entstehen.

Grundlegend für die Untersuchung der unterschiedlichen Implementierungsmöglichkeiten und der darauf folgenden Planung, wird zunächst eine Analyse des bestehenden Systems durchgeführt.

Um auf eine Migration einer Domäne bestmöglich vorbereitet zu sein, wird eine Untersuchung der verschiedenen Implementierungsmöglichkeiten erfolgen. Dabei wird auch auf die verschiedenen Thematiken wie z.B. DNS, welche mit einer Umstellung unmittelbar im Zusammenhang stehen, eingegangen. Hierfür ist des Weiteren eine Definition von Anforderungen an das neue System und Unternehmenszielen erforderlich.

Weiters wird ein Plan entworfen, welcher die wesentlichen Vor- sowie auch Nachbearbeitungsarbeiten beschreibt. Darüber hinaus werden auch Maßnahmen, welche bei Auftreten von Problemen durchzuführen sind, erarbeitet. Daraufhin wird anhand der erarbeiteten Themen ein praktischer Leitfaden, welcher bei der Umsetzung einer Migration Unterstützung bieten soll, entwickelt.

Abschließend werden noch Möglichkeiten, welche durch Einführung des neuen Systems bereits gestellt werden, beschrieben.

Abstract

Even if the operating system Microsoft Windows NT 4.0 has been getting a bit long in the tooth and is already considered as out of date, there are still environments which postpone their migration. Depending on the size of the existing domain, a conversion to a new system represents a substantial challenge for the responsible administrators.

Therefore this paper attempts to further the understanding of the requirements and effects of migration and to develop a code of practice starting with the planning of the migration and ending with the implementation.

Fundamentally for the investigation of the different implementation possibilities and the subsequent planning, an analysis of the existing system will be accomplished first. In order to be best prepared for the migration of the domain, an investigation of the different implementation possibilities will take place. Also other adjacent topics like DNS, which are directly associated with the migration, will be discussed. To achieve this, a definition of the requirements to the new system and the business objectives will be necessary.

Furthermore a plan will be developed which describes the most important preparatory as well as subsequent work. Moreover, measures which could be useful for occurring problems will be defined. Due to these developed aspects a handbook will be created which supports an administrator to successfully accomplish the implementation of such a migration.

Finally the possibilities resulting from the realisation of the migration and the introduction of the new system will be examined.

Inhaltsverzeichnis

1 Einleitung

Da Betriebsysteme durch die fortlaufende Entwicklung ständig mit verbesserter Systemleistung, neuen Sicherheitsmechanismen und erweiterten Funktionen arbeiten, sind IT-Verantwortliche ständig mit der Frage, ob eine Umstellung auf ein neueres Betriebssystem bereits notwendig ist, konfrontiert. Jedoch nur selten wird bei Herausgabe eines neuen Betriebssystems, eine Umstellung auf das neue System durchgeführt, da der Umstieg von einer Version auf die nächste oftmals nur sehr wenige Vorteile mit sich bringt. Dies führt dazu, dass nach längerer Zeit eine durchaus sehr umfangreiche Umstellung notwendig und aufgrund von zahlreichen Verbesserungen der nun übersprungenen Versionen auch gewünscht wird. Letztlich stellt auch der nach einigen Jahren eingeschränkte oder sogar eingestellte Support einer Software einen Grund für die Umstellung eines Systems dar.

Im Rahmen dieser Diplomarbeit soll die Umstellung der Domäne, der Firma Buntmetall Amstetten GmbH, welche momentan auf Windows NT 4.0 basiert, in eine auf Windows Server 2003 basierende Domäne behandelt werden. Dazu ist es notwendig den momentanen Ist-Zustand zu erheben. Um in weiterer Folge Konzepte erarbeiten zu können, gilt es die Auswirkungen auf die im Netzwerk eingesetzten Komponenten (Oracle-Cluster, Cisco Netwerkkomponenten, Faxlösung, SAN, Notes Server, Druckserver, etc.) zu untersuchen, Probleme zu erkennen und gegebenenfalls Lösungsvorschläge dafür zu erarbeiten. Bei der Konzepterstellung sollen dabei die optimalen Lösungsansätze für die Firma Buntmetall Amstetten GmbH, die alternativen Möglichkeiten sowie auch die Kompromisslösungen mit der Konzernzentrale behandelt werden.

Weiters ist zu beachten, dass eine Einbettung der Domäne der Buntmetall Amstetten GmbH in einen internationalen Konzern erfolgen muss, von dessen Konzernleitung aus es auch bestimmte Vorgaben umzusetzen gibt (z.B.: IP Netz, DHCP Server und DNS Server von Cisco). Der laufende Betrieb einer Testumgebung in welcher Probleme erkannt und Lösungen erprobt werden können, ist dabei nicht weg zu denken.

Ziel dieser Diplomarbeit ist neben der dadurch entstehenden Dokumentation auch die Aneignung von Erfahrungen mit diesen System- und Netzwerkkomponenten bei der Migration einer solchen Domäne.

Zunächst wird eine Ist-Analyse der bestehenden Infrastruktur erstellt. Weiters sind die Anforderungen an das zukünftige System zu definieren. Daraus resultiert die Frage:

- Welche Anforderungen muss das zukünftige System erfüllen?

In weiterer Folge müssen die Auswirkungen auf bestehende Komponenten erkannt werden. Daraus resultiert die Frage:

- Wie werden die bestehenden Komponenten durch eine Umstellung beeinflusst und wie sehen Lösungsansätze für die eventuell auftretenden Probleme aus?

Da es durchaus mehrere Möglichkeiten der Umsetzung der einzelnen Schritte gibt, sind Entscheidungen zu treffen, welche die Art der Umsetzung festlegen. Daraus resultiert die Frage:

- Welche Vorteile bzw. Nachteile bringen die jeweiligen Möglichkeiten der Umsetzung mit sich?

Da gewisse Vorgaben seitens der Konzernleitung zu erfüllen sind, müssen Möglichkeiten zur Umsetzung dieser Vorgaben gefunden werden. Daraus resultiert die Frage:

- Wie lassen sich die definierten Vorgaben in das zukünftige System einbinden?

Die Möglichkeiten der Umsetzung dieser Migration sollen durch eine Inhaltsanalyse von einschlägiger Fachliteratur erarbeitet werden. Um eine erfolgreiche Umsetzung der erarbeiteten Konzepte zu garantieren, müssen die erarbeiteten Lösungsansätze und die Auswirkungen auf bestehende Komponenten anschließend in einer Testumgebung praktisch erprobt werden.

2 Analyse des bestehenden Systems

Für die Migration einer Domäne ist eine tiefgehende Analyse des bestehenden Systems unabdingbar. Dabei sollen im Wesentlichen die Netzwerkinfrastruktur, die Hardwarekomponenten, die bereitgestellten Dienste und Applikationen, eingesetzte Betriebssysteme sowie die zu verwaltenden Objekte erfasst und dokumentiert werden. Eine gründliche sowie auch detaillierte Analyse des aktuellen Systems bildet die Grundlage für etwaige Entscheidungen, die für die Umstellung auf das neue System getroffen werden müssen.

2.1 Bestehende Netzwerkumgebung

Sämtliche Komponenten der aktuellen Netzwerkumgebung befinden sich innerhalb des privaten IP-Adressbereichs 10.131.0.0/16 und sind physisch über Switches miteinander verbunden. Des Weiteren sind keine Sub-Netze oder ähnliches definiert, wodurch sich sämtliche Komponenten im Netzwerk ohne zusätzliche Routing-Mechanismen erreichen können. Die Anbindung an die Konzernzentrale, welche auch den Internetzugang bereitstellt, erfolgt über einen Router und eine 2MBit/s Standleitung, welche auf MPLS (Multiprotokoll Label Switching) basiert. Diese ist mit einer 256kb/s ISDN Leitung gegen Ausfälle gesichert.

Nachfolgende Abbildung soll einen schematischen Überblick der Netzwerkinfrastruktur der vorhandenen Domäne darstellen:

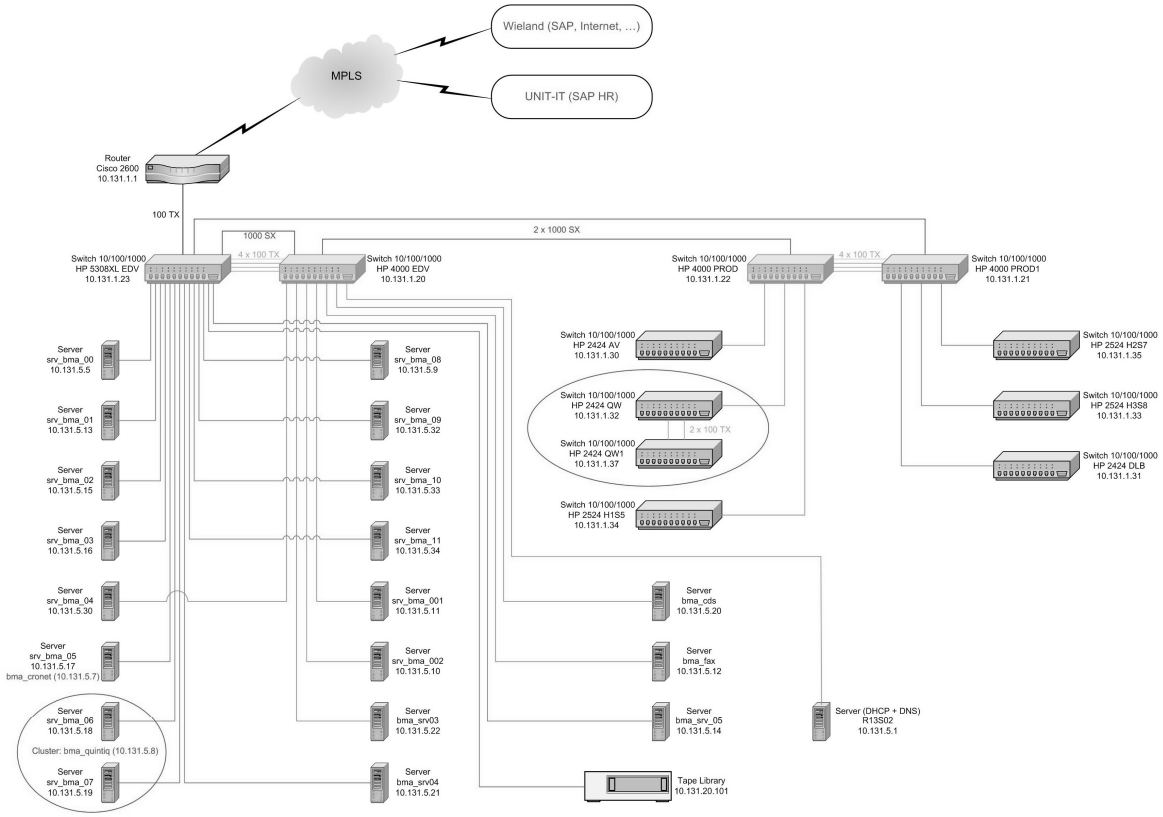

Abbildung 2.1: Schematische Darstellung der aktuellen Netzwerkumgebung

2.2 Bestehende Domänen Struktur

Das momentane Model der NT 4.0 Domäne beinhaltet am Standort lediglich eine Domäne mit dem FQDN (Full Qualified Domain Name) bma.wieland.com. Da in einer Windows NT 4.0 Umgebung aber lediglich der NetBIOS Name eine wesentliche Rolle spielt, lautet dieser vom FQDN abgeleitet BMA.

Wie in Abbildung 2.2 dargestellt, existiert seitens der Konzernleitung bereits eine Gesamtstruktur unter Microsoft Windows Server 2003 mit der Stammdomäne intern.wieland.com. Unterhalb dieser Domäne existieren mehrere (wieviele genau kann zu diesem Zeitpunkt nicht gesagt werden – dies ist aber für die Erstellung dieser Arbeit auch nicht weiter relevant) Subdomänen, unter anderem die Domäne wwag.intern.wieland.com, welche die Produktionsumgebung der Konzernleitung abbildet.

Da innerhalb der Domäne der Firma Buntmetall Amstetten GmbH auch der Zugriff auf die in Deutschland vorhandene Domäne wwag.intern.wieland.com aufgrund einer gemeinsamen Ressourcennutzung möglich sein muss, wurde mit dieser eine two-way Vertrauensstellung erstellt.

Nachfolgend eine grafische Darstellung der vorhandenen Struktur:

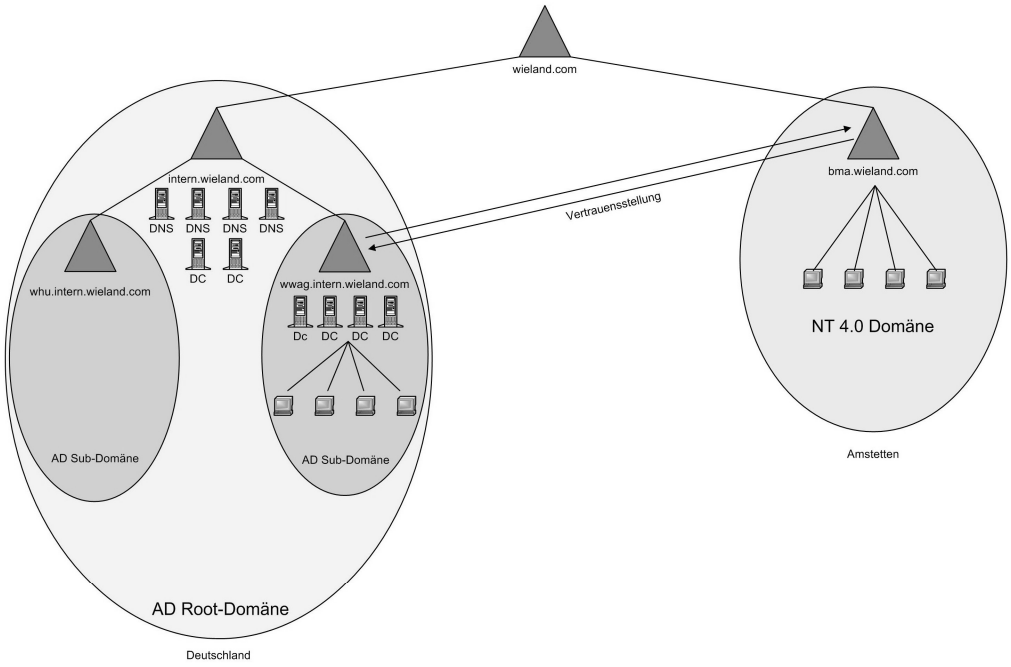

Abbildung 2.2: aktuelle Domänenstruktur

Die derzeitige Infrastruktur der Domäne besteht aus drei Domänencontroller, einem Primary Domänencontroller und zwei Backup Domänencoontroller (s. Abbildung 2.3). Der Dienst für die Replikation wurde dabei so konfiguriert, dass der PDC (Primary Domänencontroller) das Exportverzeichnis und die BDCs (Backup-Domänencontroller) die Importverzeichnisse verwalten.

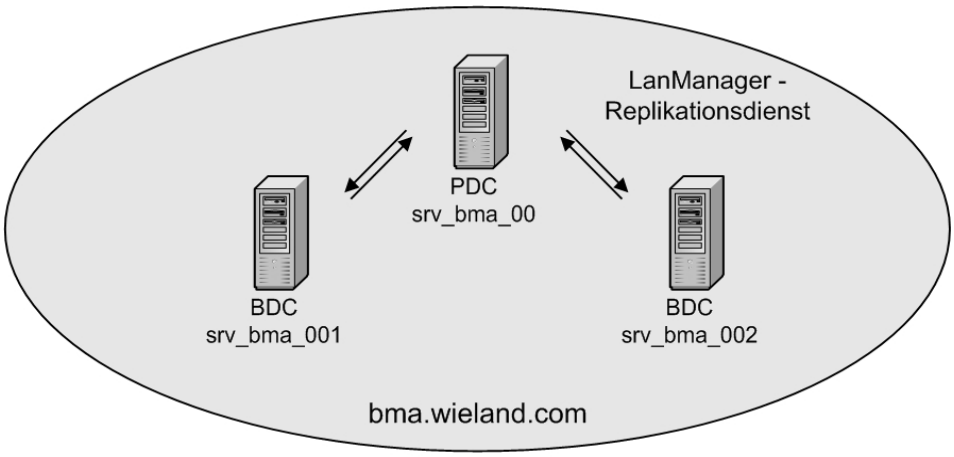

Abbildung 2.3: aktuelle Struktur am Standort

2.3 Administration der Domäne

Ein wesentlicher Punkt für den Entwurf der neuen Struktur ist eine Analyse der Verwaltung der aktuellen IT-Umgebung. Dabei sind die wesentlichsten Aufgaben der IT-Verwaltung zu erfassen.

Da die Domäne dieser Organisation nur einen Standort versorgt und sämtliche Komponenten lokal installiert sind, erfolgt die gesamte Administration zentralisiert aus der IT-Abteilung des Unternehmens. Diese umfasst die Verwaltung aller Benutzerkonten, Clientcomputer, Server für die Bereitstellung der diversen Dienste in der Domäne, Wartung und Installation von Anwendungen und die Überwachung der aktiven Netzwerkkomponenten, die für den Betrieb der gesamten Netzwerkumgebung relevant sind.

Die Administration des Gateways 10.131.1.1, der WAN Verbindung zu Wieland Werke AG in Deutschland und der Internetzugang wird hingegen durch Administratoren der Konzernzentrale in Deutschland bewerkstelligt.

2.4 Serverhardware der Domäne

Nachfolgende Tabelle umfasst sämtliche Server der Domäne bma.wieland.com und die Hardwarekomponenten welche für die Eignung für Windows Server 2003 relevant sind. Die Entscheidung ob ein Update auf Windows Server 2003 möglich ist, wurde dabei aufgrund der Daten der durchgeführten Dimensionierung mit *ADSizer*, welche in Punkt 2.5 näher beschrieben wird, getroffen.

Server	Betriebssystem RAM/CPU/Festplattenkapazität	Update auf Windows Server 2003 – DC möglich?
srv_bma_00	**Windows NT 4.0 SP6 1 x 2.40 GHz / 512 MB / 34.0 GB**	**ja**
srv_bma_01	Windows Server 2003 SE 1 x 3.40 GHz / 3.50 GB / 15.0 GB	bereits Windows 2003
srv_bma_02	Windows Server 2000 1 x 2.00 GHz / 1.0 GB / 17.0 GB	Windows 2000
srv_bma_03	Windows Server 2000 1 x 1.40 GHz / 512 MB / 17.0 GB	Windows 2000
srv_bma_04	Windows Server 2000 1 x 500 MHz / 1.5 GB / 42.0 GB	Windows 2000
srv_bma_05	Windows Server 2003 SE 1 x 2.40 GHz / 512 MB / 34.0 GB	bereits Windows 2003
srv_bma_06	Windows Server 2003 SE 1 x 2.80 GHz / 4.0 GB / 34.0 GB	bereits Windows 2003
srv_bma_07	Windows Server 2003 SE 1 x 2.80 GHz / 4.0 GB / 34.0 GB	bereits Windows 2003
srv_bma_08	Windows Server 2003 SE 1 x 3.40 GHz / 3.50 GB / 68.0 GB	bereits Windows 2003
srv_bma_09	Windows Server 2003 SE 1 x 1.00 GHz / 640 MB / 17.0 GB	bereits Windows 2003
srv_bma_10	Windows Server 2003 SE 1 x 3.40 GHz / 2.0 GB / 75.0 GB	bereits Windows 2003
srv_bma_11	Windows Server 2003 SE 1 x 3.40 GHz / 2.0 GB / 75.0 GB	bereits Windows 2003
srv_bma_001	**Windows NT 4.0 SP6 1 x 266 MHz / 160 MB / 4.0 GB**	**nein**
srv_bma_002	**Windows NT 4.0 SP6 1 x 400 MHz / 512 MB / 4.0 GB**	**nein**
bma_srv04	Windows NT 4.0 SP6 1 x 1.00 GHz / 256 MB / 8.0 GB	nein
bma_srv05	Windows Server 2000 1 x 1.00 Ghz / 640 MB / 4.0 GB	Windows 2000
bma_fax	Windows NT 4.0 SP6 1 x 299 MHz / 160 MB / 4.0 GB	nein
bma_cds	CD-Rom Archiv Server	nein (eigenes System)
r13s02	Windows Server 2000 1 x 1.60 GHz / 256 MB / 3.0 GB	Windows 2000

Tabelle 2.1: Hardware- u. Softwarekomponenten der vorhandenen Server

2.5 Anforderungen an die neue Serverhardware

Für die Festlegung ob ein Update auf Windows Server 2003 möglich ist, werden von Microsoft folgende Parameter vorgegeben:

Komponente	Erfordernis
CPU	Mind. 133 MHz, empfohlen 550 MHz und höher
RAM	Mind. 128 MB, empfohlen 256 MB (4 GB Maximum)
Festplatte	1.25 – 2.00 GB freier Speicherplatz
Laufwerk	CD-Rom od. DVD-Rom

Tabelle 2.2: Hardwareanforderungen lt. Microsoft

Bei diesen Daten handelt es sich aber lediglich um die Mindestanforderungen für die Installation von Microsoft Windows Server 2003 und nicht um Vorgaben zum Betrieb von Active Directory. Somit muss beachtet werden, dass mit dem Anstieg der zu verwaltenden Objekte auch ein Anstieg der Rechnerauslastung einhergeht. Aus diesem Grund hat Microsoft mit Windows 2000 ein Tool zur Berechnung der notwendigen Serverkapazität in Abhängigkeit von Active Directory spezifischen Daten herausgegeben. Obwohl dieses Tool für Windows 2000 konzipiert wurde, ist es dennoch sinnvoll eine Berechnung für Windows Server 2003 durchzuführen. Mit dem Tool *ADSizer* ist es möglich Parameter wie z.B. Anzahl der User, Computer oder sonstige zu verwaltenden Objekte, Verwendung von Active Directory integriertem DNS oder Microsoft Exchange, sowie das durchschnittliche Administrationsaufkommen anzugeben und anschließend die Berechnung der ungefähren Größe des Globalen Katalogs durchzuführen. In weiterer Folge wird auch eine Abschätzung der erforderlichen Serverkomponenten wie Prozessorleistung, benötigter Arbeitsspeicher oder die Festplattenkapazität erstellt.

Für die Auswertung ist es sinnvoll Reserven einzuplanen um mit den Serverkapazitäten auch für das zukünftige Wachstum gerüstet zu sein. Für die Dimensionierung der zukünftigen Domänencontroller wurde somit die aktuelle Anzahl von Usern und Computer verdoppelt. Weitere Angaben wie z.B. die Gruppenabhängigkeiten von Usern wurden entweder geschätzt oder die vorgeschlagenen Werte des Programms herangezogen, da diese ohnehin für Domänen größeren Ausmaßes gerechnet wurden.

Die zugrunde liegenden Parameter für die Abschätzung mit dem Programm *ADSizer* wurden dem Punkt 2.11 entnommen.

Nachfolgend zwei Grafiken, die den Output dieses Tools darstellen:

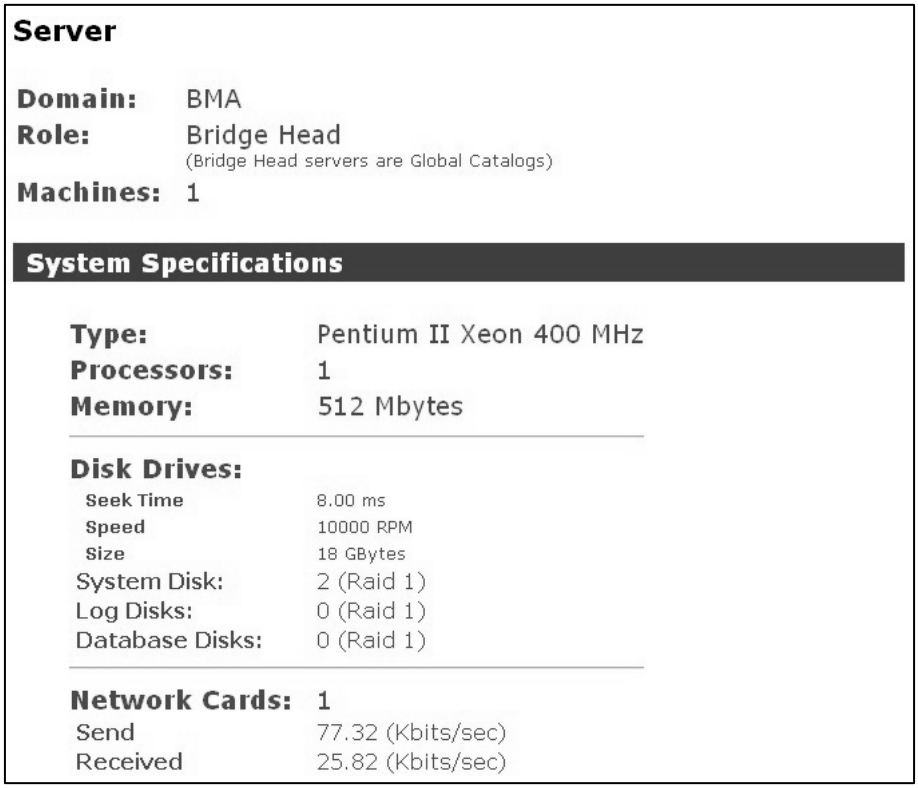

Abbildung 2.4: Ausgabe 1 des Tools ADSizer

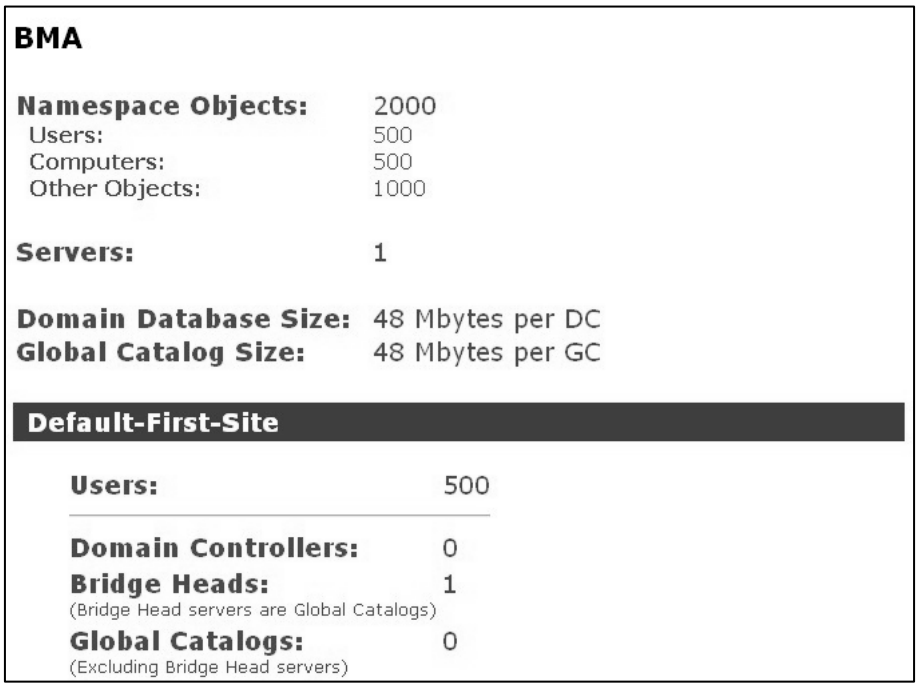

Abbildung 2.5: Ausgabe 2 des Tools ADSizer

Wie auf diesen Abbildungen zu erkennen ist, kommt es aufgrund der noch relativ geringen Größe dieser Domäne zu keinen besonderen Erfordernissen an die zukünftigen Domänencontroller. Somit sind bei der Bemessung der Server keine wesentlichen Aspekte zu beachten, da die Erfordernisse ohnehin von nahezu allen aktuellen Systemen erfüllt werden können, insofern für die neuen Domänencontroller auch neue Systeme bereitgestellt werden. Soll die bestehende Hardware weiterverwendet werden, so bietet diese Dimensionierung auch die Entscheidungsgrundlage ob dies überhaupt möglich ist.

2.6 Dienste und Anwendungen der Domäne

Nachstehende Tabelle soll einen Überblick über die Funktionen bzw. Dienste, welche auf den einzelnen Server implementiert sind, geben:

Server	Server-Funktion	Dienste und Anwendungen
srv_bma_00	**PDC**	**WINS, LMRepl-Exportserver, NTP Server**
srv_bma_01	Mitgliedsserver	Lotus Notes Server
srv_bma_02	Mitgliedsserver	Cronet Test Instanz
srv_bma_03	Mitgliedsserver	Software Verteilung CCM
srv_bma_04	Mitgliedsserver	Quintiq Test Instanz
srv_bma_05	Mitgliedsserver	Druckserver, Schnittstelle zu SAP, RAS Server
srv_bma_06	Mitgliedsserver	Mitgliedsserver Oracle Cluster – Quintiq Instanz
srv_bma_07	Mitgliedsserver	Mitgliedsserver Oracle Cluster – Cronet Instanz
srv_bma_08	Mitgliedsserver	Quintiq Server, Cronet Client
srv_bma_09	Mitgliedsserver	Test-Server
srv_bma_10	Mitgliedsserver	MRS Fax Server
srv_bma_11	Mitgliedsserver	Easy Archiv Server
srv_bma_12	Mitgliedsserver	MicroTrend Server (Virenscanner)
srv_bma_001	**BDC**	**LMRepl-Importserver**
srv_bma_002	**BDC**	**LMRepl-Importserver**
bma_srv04	Mitgliedsserver	Chrystal Reports Server, Microsoft IIS Server
bma_srv05	Mitgliedsserver	Datei Server
bma_fax	Mitgliedsserver	alter Fax Server, SMTP Gateway

Tabelle 2.3: Dienste und Anwendungen der vorhandenen Server

Server	Server-Funktion	Dienste und Anwendungen
bma_cds	Mitgliedsserver	CD-Rom Server
r13s02	Mitgliedsserver	DHCP und DNS Server (Cisco Network Registrar 5.5.9)

Tabelle 2.3 (Fortsetzung): Dienste und Anwendungen der vorhandenen Server

2.7 Netzwerkkonfiguration der Domänencontroller

Name DC	Netzwerkkarte	IP-Adresse	Subnetz-maske	Standard-gateway
srv_bma_00	Compaq NC7781 Gigabit Server Adapter	10.131.5.5	255.255.0.0	10.131.1.1
srv_bma_001	Compaq Netflex-3 Driver, Version 4.25m SP4	10.131.5.11	255.255.0.0	10.131.1.1
srv_bma_002	Compaq Netflex-3 Driver, Version 4.25m SP4	10.131.5.10	255.255.0.0	10.131.1.1

Tabelle 2.4: Netzwerkkonfiguration der Domänencontroller

2.8 Serverfunktionen der Domänencontroller in der neuen Umgebung

Name DC	Erfüllt Hardware-voraussetzungen	Funktion vor Update	Funktion nach Update
srv_bma_00	Ja	Windows NT 4.0 PDC	Windows Server 2003 DC
srv_bma_001	Nein	Windows NT 4.0 BDC	Rollback-Server
srv_bma_002	Nein	Windows NT 4.0 BDC	Rollback-Server

Tabelle 2.5: Funktion der Domänencontroller in der neuen Umgebung

Wie in Tabelle 2.1 dargestellt, ist aufgrund der veralteten Hardwarekomponenten der BDCs (srv_bma_001, srv_bma_002) ein Update auf Windows Server 2003 auf diesen Rechnern nicht möglich. Deshalb werden diesen nach der Aktualisierung keine besonderen Funktionen mehr zugewiesen. Da für einen Wiederherstellungsplan (s. Punkt 6.2) ohnehin ein BDC offline genommen werden soll, wird den Servern srv_bma_001 und srv_bma_002 die Rolle des Rollback-Servers zugewiesen. Bei erfolgreicher Migration werden aber auch diese keine Funktion in der neuen Domäne einnehmen und somit nach der Migration außer Betrieb genommen.

2.9 DHCP-Dienst in der aktuellen Umgebung

Der im Moment laufende DHCP Dienst wird auf dem Server r13s02.bma.wieland.com mittels Cisco Network Registrar 5.5.9 bereitgestellt. Die Konfiguration sieht dabei folgendermaßen aus:

Netzwerkbereich:	10.131.0.0
Subnet Mask:	255.255.0.0
Adresspool:	10.131.10.1 – 10.131.12.255

Tabelle 2.6: Auszug 1 der Konfiguration des DHCP-Dienstes

Reservations:	10.131.10.1	00:40:ca:85:c2:10	wwag-bma-119-63.bma.wieland.com
	10.131.10.2	00:00:86:5d:c1:b7	bma2716-000.bma.wieland.com
	10.131.10.10	00:01:02:1f:ae:10	BMA031.bma.wieland.com
	10.131.10.15	00:40:ca:7b:e0:bd	bma2851-097.bma.wieland.com
	10.131.12.91	00:40:ca:5e:4a:ad	bma2851-077.bma.wieland.com
	10.131.20.1	02:00:cc:00:11:6e	BMA-NB99.bma.wieland.com

Tabelle 2.7: Auszug 2 der Konfiguration des DHCP-Dienstes

Dynamische Updates durchführen:	aktiviert	
Forward DNS:	bma.wieland.com	10.131.5.1
Reverse DNS:	131.10.in-addr.arpa	10.131.5.1
Zuweisung eines Hostnamen (wenn keiner zugewiesen wurde):	wwag-bma	

Tabelle 2.8: Auszug 3 der Konfiguration des DHCP-Dienstes

Domänen-Name:	bma.wieland.com
DNS-Server:	10.131.5.1 (lokaler DNS Server)
	10.66.5.2
	10.66.5.1
MCNS-Security-Server:	10.131.5.16
NetBIOS-Server:	10.131.5.5
NetBIOS-Type:	8
Routers:	10.131.1.1
TFTP-Server:	10.131.5.1
Lease Time:	86400

Tabelle 2.9: Auszug 4 der Konfiguration des DHCP-Dienstes

2.10 DNS-Dienst in der aktuellen Umgebung

Auch der DNS-Dienst der momentanen Netzwerkumgebung wird auf dem Server r13s02.bma.wieland.com mittels Cisco Network Registrar 5.5.9 bereitgestellt. Die Konfiguration sieht dabei folgendermaßen aus:

Forwarders:	10.34.5.1
	10.66.5.1
	10.34.5.2
Rekursive Abfrage:	aktiviert
Round-Robin:	aktiviert
Subnet Sorting:	deaktiviert
Incremental Zone Transfers:	aktiviert
Notify:	aktiviert

Tabelle 2.10: Konfigurierte Optionen des DNS Servers

	Zone	Primärer DNS-Server	Weitere DNS-Server
Primäre Zonen:	bma.wieland.com	r13s02.bma.wieland.com	r01s72.intern.wieland.com
			r01s73.intern.wieland.com
			r01s74.intern.wieland.com
			r01s75.intern.wieland.com
	131.10.in-addr.arpa	r13s02.bma.wieland.com	
Sekundäre Zonen:	ecm.wieland.com	10.66.5.1	
	intern.wieland.com	10.34.5.1	
	wwag.intern.wieland.com	10.34.5.1	
	wwag.wieland.com	10.34.5.1	
	34.10.in-addr.arpa	10.34.5.1	
	36.10.in-addr.arpa	10.34.5.1	
Akzeptiert dynamische Updates von:	10.131.5.1		
	127.0.0.1		

Tabelle 2.11: Konfiguration der DNS Zonen

2.11 WINS-Dienst der aktuellen Umgebung

Wie in Punkt 2.6 beschrieben, ist der WINS (Windows Internet Naming Service) auf dem momentanen primären Domänencontroller srv_bma_00 implementiert. Dieser erfüllt in Netzwerken mit Windows NT 4.0 die wesentliche Aufgabe der Namensauflösung. Die Konfiguration dieses Dienstes umfasst keine Abweichungen von den Standardeinstellungen, da dieser Server lediglich für die Replikation mit dem Server r01s75.intern.wieland.com (10.66.5.1) in der Konzernzentrale in Deutschland konfiguriert wurde. Sämtliche in der Domäne der Firma Buntmetall Amstetten GmbH befindlichen Clients verwenden diesen Server als primären WINS-Server.

2.12 Aktuelle Domänen Objekte

Für eine erfolgreiche Umstellung der Domäne auf Microsoft Windows Server 2003 ist eine Analyse der zu verwaltenden Objekte notwendig. Die dadurch gewonnenen Parameter können auch für eine Abschätzung der erforderlichen Hardwarekomponenten mit dem Tool *ADSizer* herangezogen werden. Weiters sollen mit Hilfe dieser Analyse veraltete und nicht mehr benötigte Objekte erkannt werden, um diese nicht sinnloserweise in die neue Struktur zu übernehmen.

2.12.1 Benutzerkonten

Die Analyse der Domänencontroller hat eine Anzahl von 212 Benutzerkonten ergeben. Diese werden in einem eigenen Dokument aufgelistet und müssen auf ihre Aktualität überprüft werden. Dies ist mit Hilfe des Befehls **usrstat.exe**, welcher das Datum des letzten Logins jedes einzelnen Users ausgibt, aus dem Windows 2000 Resource Kit möglich.

2.12.2 Gruppenkonten

Die Analyse der Domänencontroller hat eine Anzahl von 94 Gruppenkonten ergeben. Diese werden in einem eigenen Dokument aufgelistet und müssen auf ihre Aktualität überprüft werden.

2.12.3 Clientumgebung - Computerkonten

Die Umgebung der Clients umfasst ca. 150 PCs. Diese sind bereits zum größten Teil mit dem Betriebssystem Windows XP Professional inkl. Service Pack 1 ausgestattet. Es existieren jedoch auch Clientrechner, welche mit älteren Windows Versionen ausgerüstet sind. Diese, vor allem in der Produktion (aufgrund der geringen Anforderungen) eingesetzten PCs, laufen noch unter dem Betriebssystem Windows NT 4.0 inkl. Service Pack 6a. Da aber auch Clientrechner unter Windows NT 4.0 inkl. Service Pack ab Version 3 in einer Active Directory Umgebung mit Einschränkungen betrieben werden können, sind keine zusätzlichen Maßnahmen zur Integration nicht unterstützter Betriebssysteme in Active Directory notwendig.

Die Server der aktuellen Umgebung sind zum größten Teil bereits mit Windows Server 2003 ausgestattet (s. Tabelle 2.1). Dennoch ist es nicht Ziel dieser Arbeit sämtliche Server auf Windows Server 2003 umzustellen, sondern die Domäne nach Windows Server 2003 zu migrieren, wodurch lediglich die Domänencontroller behandelt werden müssen.

2.12.4 Systemrichtlinien

Die Analyse der Domänencontroller hat eine Anzahl von 29 Systemrichtlinien ergeben. Diese werden in einem eigenen Dokument aufgelistet und müssen auf ihre Aktualität überprüft werden.

2.13 Datei- und Druckinfrastruktur

Wie in Tabelle 2.3 dargestellt, sind die Funktionen des Datei- und Druckservers bereits auf neueren Betriebssystemen als Windows NT 4.0 implementiert. Dadurch entstehen für die Migration der Domäne von Windows NT 4.0 nach Windows Server 2003 keine Anforderungen bzw. Aufgaben hinsichtlich der Datei- und Druckinfrastruktur.

3 Active Directory Design

Bevor die Planung der Migration begonnen werden kann, ist es notwendig das zu realisierende Active Directory Modell zu planen. Hierbei sollen sämtliche Möglichkeiten der Einführung von Active Directory in Betracht gezogen werden, um aufgrund von diversen Vor- und Nachteilen jenes Modell zu finden, womit die bestmögliche Abbildung der Organisation und die effizienteste Anpassung an die Unternehmensziele erreicht werden kann.

3.1 Gesamtstrukturen

„Die Active Directory-Infrastruktur bietet notwendigerweise einen - wenn auch eingeschränkten - Überblick über die Gesamtstruktur. Dies ermöglicht Administratoren der Stammdomäne der Gesamtstruktur die Verwaltung von Schemadaten, Konfigurationsdaten und Domänencontroller. Die diesen Administratoren eingeräumten Möglichkeiten bergen jedoch auch ein gewisses Gefahrenpotenzial. Ist darüber hinaus eine Autonomie oder Trennung wichtig, so ist das Sicherheitsniveau einer einzelnen Domäne möglicherweise nicht ausreichend. Vor allem in großen Unternehmen kann es organisatorische, rechtliche oder betriebliche Anforderungen geben, die eine Aufteilung der ad-

ministrativen Kontrolle auf eigenständige Gesamtstrukturen zwingend erforderlich machen. " (Microsoft, 2006 a)

Da im Fall der Firma Buntmetall Amstetten GmbH bereits eine Gesamtstruktur mit Active Directory in der Konzernzentrale in Deutschland vorhanden ist, muss eine Entscheidung getroffen werden, welche festlegt ob die geplante Domäne in diese Gesamtstruktur eingebettet werden soll oder ob eine eigene Gesamtstruktur erstellt werden soll. Dafür ist eine genaue Analyse der Vor- und Nachteile, welche durch Implementierung einer eigenen bzw. Integration in eine bestehende Gesamtstruktur einhergehen, notwendig.

3.1.1 Aufbau mehrerer Gesamtstrukturen

„Bei Microsoft Windows NT 4.0 ist die Domäne die ultimative Komponente. Sie ist klar abgegrenzt und wird getrennt verwaltet. Mit der Einführung von Active Directory unter Microsoft Windows 2000 wurde die neue Kategorie der Gesamtstruktur eingeführt, die sich auf Dienste und Daten aller Domänen auswirkt.

Die Verfügbarkeit des Verzeichnisdienstes und die Trennung oder Autonomie der Daten in einer Active Directory-Domäne hängen nicht nur vom Administrator der betreffenden Domäne und den Administratoren der Gesamtstruktur ab, sondern auch von anderen Domänenadministratoren innerhalb der Gesamtstruktur." (Microsoft, 2006 a)

Aufgrund der in den vorangegangenen Absätzen beschriebenen Abhängigkeit von der Stammdomäne, kann die Errichtung einer eigenen Gesamtstruktur für notwendig erachtet werden. Damit ist es möglich das Netzwerk aus Gründen der Unabhängigkeit in der Verwaltung zu unterteilen und somit die Möglichkeit zu schaffen, Verzeichnisdienste unabhängig voneinander oder Daten und Dienste ohne Störungsgefahr zu verwalten. (vgl. Microsoft, 2006 a)

Da jede Gesamtstruktur separat verwaltet wird, muss jedoch auch berücksichtigt werden, dass mit dem Entwurf einer eigenen Gesamtstruktur und der damit einhergehenden administrativen Unabhängigkeit der Verwaltungsaufwand für die Organisation steigt und damit Kosten verbunden sind. Somit ist es wichtig einen sinnvollen Ausgleich zwischen Autonomie oder Trennung im Gegensatz zu Interoperabilität und Zusammenarbeit zu finden. (vgl. Microsoft, 2006 a)

In Active Directory sind Möglichkeiten implementiert, um eine Delegierung der einzelnen Verwaltungsbereiche vorzunehmen. Dies kann dabei auf mehreren Ebenen erfolgen. Diese Ebenen beinhalten Gesamtstrukturen, Domänen und Organisationseinheiten. (vgl. Microsoft, 2006 a)

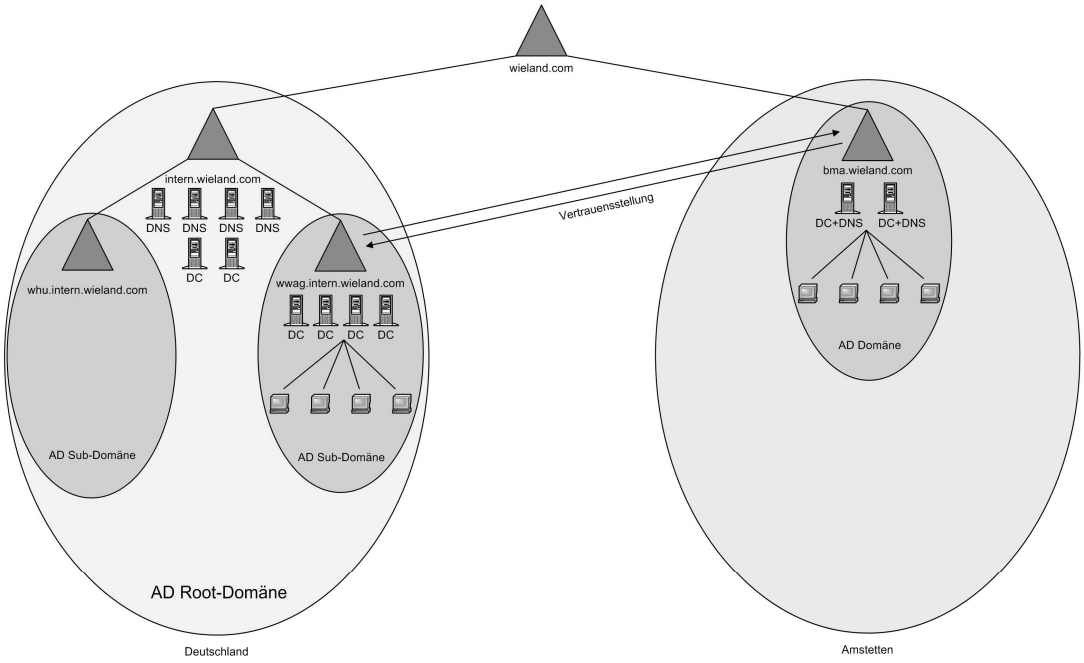

Abbildung 3.1: Erstellung der neuen Domäne als eigene Gesamtstruktur

Oftmals sind die Aufteilung der Verwaltung und eine somit angemessene Verwaltungsrechtevergabe innerhalb einer einzelnen Gesamtstruktur unter Zuhilfenahme der Delegierungsmöglichkeiten ausreichend. Es gibt allerdings Anforderungen, wodurch eine solche Delegierung als unzulänglich betrachtet wird. Nachfolgend erfolgt eine Auflistung der möglichen Aspekte, die zu einer Aufteilung in mehrere Gesamtstrukturen führen können:

- Dienstautonomie

  Darunter versteht man die unabhängige Verwaltung von Schema- und Konfigurationscontainer in einer Active Directory Umgebung. Dies kann dann erforderlich werden, wenn ein Unternehmensbereich eine Anwendung mit Verzeichnisdienstunterstützung, welche eine Schemaerweiterung erfordert, implementieren möchte und dies unabhängig von einer Entscheidung der höher stehenden IT-Organisation durchführen möchte. (vgl. Microsoft, 2006 a)

- Diensttrennung

  Hierbei soll die Sicherheit geschaffen werden, dass kein Administrator außerhalb der eigenen Verwaltungsstruktur den Betrieb des Verzeichnisdienstes beeinflussen kann. Dies kann dann erforderlich werden, wenn ein Domänencontroller außerhalb des eigenen Einflussbereichs aufgestellt werden muss und die Sicherheit dieses Domänencontrollers nicht gewährleistet werden kann. Hier würde eine Erstellung einer von der Unternehmensgesamtstruktur getrennten, eigenen Gesamtstruktur eine mögliche Lösung darstellen. (vgl. Microsoft, 2006 a)

- Datentrennung

  Dieser Punkt beschreibt die Sicherheit, dass Administratoren anderer Domänen auf Daten eines Domänencontrollers oder Mitgliedsrechner Zugriff erlangen können. Dies stellt besonders in Unternehmen, welche mit der Verwaltung von wesentlich vertrauenswürdigen Daten konfrontiert sind, eine besondere Problematik dar. (vgl. Microsoft, 2006 a)

- Abgrenzung der Verzeichnisreplikation

  Hierbei kann die Einschränkung des Replikationsverkehrs, welcher oftmals über langsame WAN-Verbindung erfolgen muss, geschaffen werden. Auswirkungen von gesamtstrukturweiten Änderungen haben somit keinen Einfluss auf andere Gesamtstrukturen.

- Entwicklungs- und Testumgebungen

  Um eine effiziente Abschottung von Entwicklungs- und Testumgebungen zu implementieren und einen störungsfreien Betrieb der Produktionsumgebung zu gewährleisten, kann ebenfalls die Erstellung einer eigenständigen Gesamtstruktur in Erwägung gezogen werden.

3.1.1.1 Gesamtstrukturvertrauensstellungen

Um im Fall der Errichtung einer eigenen Gesamtstruktur auch die notwendigen Zugriffe auf andere Gesamtstrukturen zu ermöglichen, wurde mit Windows Server 2003 die Funktion von Gesamtstrukturvertrauensstellungen eingeführt. Mit Hilfe einer Windows Server 2003 Gesamtstrukturvertrauensstellung ist es möglich zwei getrennte Gesamtstrukturen durch unidirektionale oder bidirektionale transitive Vertrauensstellungen zu verknüpfen. Eine bidirektionale

Gesamtstrukturvertrauensstellung erstellt somit transitive Vertrauensstellungen zwischen jeder Domäne in beiden Gesamtstrukturen. (vgl. Microsoft, 2006 b)

Nachfolgend werden die Vorteile von Gesamtstrukturvertrauensstellungen aus Gründen der Vollständigkeit angeführt (Microsoft, 2006 b):

- Vereinfachte Ressourcenverwaltung in zwei Windows Server 2003 Gesamtstrukturen durch Reduzieren der zum Freigeben der Ressourcen erforderlichen Anzahl externer Vertrauensstellungen
- Vollständige bidirektionale Vertrauensstellungen mit jeder Domäne in beiden Gesamtstrukturen
- Verwendung der gesamtstrukturübergreifenden Authentifizierung von Benutzerprinzipalnamen
- Verwendung der Kerberos V5- und NTLM-Authentifizierungsprotokolle, um die Vertrauenswürdigkeit der zwischen Gesamtstrukturen übertragenen Autorisierungsdaten zu optimieren
- Flexible Verwaltung - Verwaltungsaufgaben können für jede Gesamtstruktur unterschiedlich sein

Es ist jedoch zu beachten, dass zwei Gesamtstrukturen, welche eine solche Gesamtstrukturvertrauensstellung aufbauen, zwei wesentliche Active Directory Ressourcen nicht gemeinsam nutzen. Diese sind das Active Directory Schema und der globale Katalog. Dies hat zur Folge, dass Änderungen, welche am Schema der einen Gesamtstruktur vorgenommen werden, nicht automatisch auf das Schema der anderen Gesamtstruktur übertragen werden. Dies stellt aber in der Regel kein besonderes Problem dar, da diese Änderungen lediglich auch in der zweiten Gesamtstruktur manuell durchgeführt werden müssen.

Wesentlich problematischer hingegen ist jedoch, dass kein domänenübergreifender Globaler Katalog der jeweiligen Gesamtstrukturen existiert. Der GC (Global Catalog) ermöglicht den Benutzern ein Auffinden von Benutzern, Gruppen und diversen Ressourcen in anderen Domänen. Somit ist es bei Fehlen eines gemeinsamen Globalen Katalogs notwendig, dass Benutzer wissen in welcher Gesamtstruktur sich die benötigen Ressourcen befinden, um diese zu erreichen. Da sich bei der Firma Buntmetall Amstetten GmbH der domänen-

übergreifende Zugriff auf Ressourcen jedoch lediglich auf die Authentifizierung für den Internetzugriff beschränkt, stellt diese Problematik kein wesentliches Entscheidungskriterium dar.

„Gesamtstrukturvertrauensstellungen können nur zwischen zwei Gesamtstrukturen erstellt werden und können nicht implizit auf eine dritte Gesamtstruktur erweitert werden. Wenn also eine Gesamtstrukturvertrauensstellung zwischen der Gesamtstruktur 1 und 2 und eine Gesamtstrukturvertrauensstellung zwischen der Gesamtstruktur 2 und 3 erstellt wird, weist die Gesamtstruktur 1 keine implizite Vertrauensstellung mit der Gesamtstruktur 3 auf." (Microsoft, 2006 b)

3.1.1.2 Externe Vertrauensstellungen

Für den Fall, dass Benutzer einer Windows Server 2003 Gesamtstruktur Zugriff auf Ressourcen in einer Domäne einer anderen Gesamtstruktur benötigen, kann dies auch mit einer externen Vertrauensstellung ermöglicht werden. Diese Art von Vertrauensstellung kann unidirektional oder bidirektional eingerichtet werden und ist nicht transitiv, d.h. sie ermöglicht untergeordneten Domänen nicht automatisch den Zugriff auf jene Domäne mit welcher die Vertrauensstellung aufgebaut wurde.

Diesen Typ von Vertrauensstellungen erhalten sämtliche Vertrauensstellungen, welche unter Windows NT 4.0 erstellt wurden und während einer Inplace Migration erhalten bleiben. Dies ist auch ein wesentlicher Punkt für die Durchführung der Migration der Umgebung der Firma Buntmetall Amstetten GmbH, da die Vertrauensstellung für die Authentifizierung der Benutzer für den Internetzugang zwingend erforderlich ist.

„Standardmäßig wird für neue externe Vertrauensstellungen und Gesamtstrukturvertrauensstellungen in Active Directory unter Betriebssystemen der Windows Server 2003-Produktfamilie die SID-Filterung erzwungen. Die SID-Filterung wird verwendet, um Angriffen von zerstörerischen Benutzern vorzubeugen, die versuchen, einem anderen Benutzerkonto erhöhte Benutzerrechte zu erteilen. Das Erzwingen der SID-Filterung für Gesamtstrukturvertrauensstellungen verhindert nicht das Migrieren in Domänen innerhalb derselben Gesamtstruktur mithilfe des SID-Verlaufs und hat keine Auswirkungen auf Ihre Zugriffssteuerungsstrategie für universelle Gruppen." (Microsoft, 2006 b)

3.1.2 Integration in eine bestehende Gesamtstruktur

Aufgrund diverser Anforderungen kann die Integration in die bestehende Gesamtstruktur in Betracht gezogen werden. Dies hat den Vorteil, dass auch jene Funktionen, welche in Verbindung mit Gesamtstrukturen unter Windows Server 2003 implementiert wurden, für Anwendungen welche Active Directory nutzen verfügbar sind.

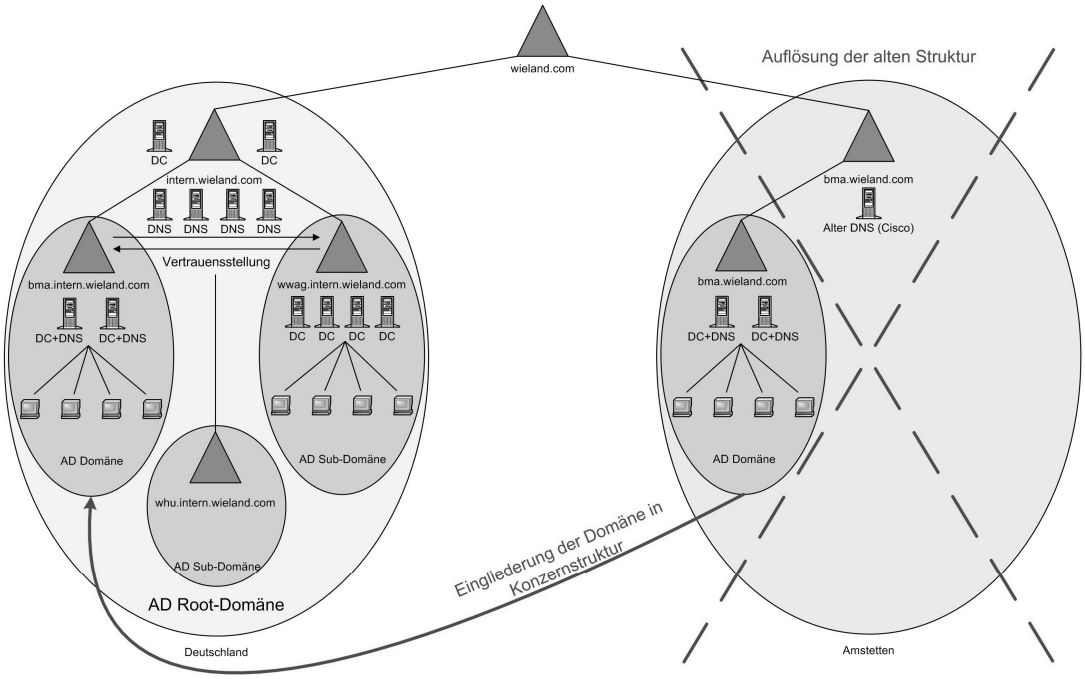

Abbildung 3.2: Integration der neuen Domäne in die bestehende Gesamtstruktur

Für die Entscheidung, ob innerhalb einer bestehenden Gesamtstruktur eine neue Domäne eingerichtet werden soll, müssen verschiedene Faktoren in Betrachtung gezogen werden. So sind zum Beispiel alle Vertrauensstellungen zwischen den Domänen einer Gesamtstruktur beidseitig und transitiv. Diese werden zudem auch noch bei der Erstellung der jeweiligen Domäne automatisch eingerichtet. Hier kommt noch hinzu, dass der Zugriff der Administratorgruppe der Stammdomäne für jede erstellte Domäne standardmäßig implementiert wird, also die Zugriffsberechtigungen automatisch der Gruppe „Enterprise Admins" zugeordnet werden. (vgl. Netigator, 2006 a)

„Schließlich ist es zwar offiziell so, dass die Administratoren einer Domäne keine inhärenten Berechtigungen in anderen Domänen der Gesamtstruktur besitzen, aber in AD existiert eine Schwachstelle, die bei entsprechender Ausnutzung dazu führen kann, dass der Administrator einer Domäne

Administratorrechte in einer anderen Domäne dieser Gesamtstruktur erhält." (Netigator, 2006 a)

Wie schon oben erwähnt, ergibt sich durch diese Lösung jedoch auch eine gewisse Abhängigkeit von der Stammdomäne, da Bestandteile des Active Directory wie Schemapartition, Konfigurationspartition und Globaler Katalog nur einmal gesamtstrukturweit existieren und dort auch konfiguriert werden. Üblicherweise werden diese Funktionen bei Erzeugung des ersten Domänencontrollers in der ersten Domäne (Stammdomäne) von diesem übernommen.

Die Abhängigkeit von der Stammdomäne entsteht aber nicht ausschließlich durch die gesamtstrukturweiten Aufgaben von diesen Active Directory Komponenten, sondern auch durch die Anwendung von Gruppenrichtlinien. Diese können nämlich auf Standorte verlinkt werden und somit Vorgaben für diese Domäne (Standort) schaffen.

In den nächsten beiden Punkten wird auf diese Einschränkungen näher eingegangen.

3.1.2.1 Gruppenrichtlinien auf Standortebene

Mit Hilfe von auf Standorte verlinkten Gruppenrichtlinien ist ein sehr tiefer Eingriff in einen Standort möglich. Auf diese Weise können sehr einschränkende Vorgaben wie z.B. Softwareinstallationen, Logon-Skripte, etc. konfiguriert werden. Vorgaben bezüglich der Konten- und Kennwortrichtlinien können hingegen nicht konfiguriert werden, da die Kontenadministration ausschließlich lokal innerhalb der Domäne stattfindet.

3.1.2.2 Enterprise-Administratoren

Die Administration der gesamtstrukturweiten Aufgaben erfolgt durch die Gruppe der Enterprise-Administratoren. Diese werden standardmäßig bei Installation einer neuen Domäne auch Mitglied der Administratoren-Gruppe in der erzeugten Domäne. Somit haben diese auch vollen Zugriff auf diese neue Domäne. Dies lässt sich aber durch Entfernen der Enterprise-Administratoren aus der Administratoren Gruppe verhindern. Da in unserem Fall die Gruppe der Enterprise-Administratoren von der Konzernleitung verwaltet wird und Eingriffe in die geplante Domäne nicht möglich sein sollen, muss dies auch hier zur Anwendung kommen.

3.2 Funktionalität von Gesamtstruktur- und Domänenebene

Um eine einwandfreie Kommunikation zwischen verschiedenen Domänencontroller zu gewährleisten, ist eine nach gewissen Kriterien gewählte Funktionsebenenkonfiguration ausschlaggebend. Somit müssen, vor der Erstellung von Gesamtstrukturen und Domänen, zunächst Überlegungen bezüglich der notwendigen Funktionsebene stattfinden. Die Wahl der letztendlichen Konfiguration hängt dabei wesentlich von den eingesetzten Betriebssystemen ab.

3.2.1 Gesamtstrukturfunktionsebenen

Die Gesamtstrukturfunktionsebene definiert die gesamtstrukturweiten Funktionen von Active Directory innerhalb der Netzwerkumgebung.

Die nachfolgende Tabelle soll einen Überblick der unterstützten Domänencontroller in Abhängigkeit der konfigurierten Gesamtstrukturfunktionsebene darstellen:

Gesamtstrukturfunktionsebene	Unterstützte Domänencontroller
Windows 2000 (Standard)	Windows NT 4.0 Windows 2000 Windows Server 2003-Produktfamilie
Windows Server 2003-interim	Windows NT 4.0 Windows Server 2003-Produktfamilie
Windows Server 2003	Windows Server 2003-Produktfamilie

Tabelle 3.1: Gesamtstrukturfunktionsebenen in Windows Server 2003 (Microsoft, 2006 e)

Die folgende Tabelle stellt die Verfügbarkeit der einzelnen Funktionen in Anhängigkeit der Gesamtstrukturfunktionsebene dar:

Gesamtstrukturfunktion	Windows 2000	Windows Server 2003
Verbesserte Replikation des globalen Katalogs	Aktiviert, falls Replikationspartner Windows Server 2003 verwenden	Aktiviert
Funktionsschemaobjekte	Deaktiviert	Aktiviert
Gesamtstrukturvertrauensstellungen	Deaktiviert	Aktiviert
Verknüpfte Wertreplikation	Deaktiviert	Aktiviert

Tabelle 3.2: AD-Features in Abhängigkeit der Gesamtstrukturfunktionsebene (Microsoft, 2006 e)

Gesamtstrukturfunktion	Windows 2000	Windows Server 2003
Domänenumbenennung	Deaktiviert	Aktiviert
Verbesserte Active Directory-Replikationsalgorithmen	Deaktiviert	Aktiviert
Dynamische Erweiterungsklassen	Deaktiviert	Aktiviert
"objectClass"-Änderung für das "InetOrgPerson"-Attribut	Deaktiviert	Aktiviert

Tabelle 3.2 Fortsetzung: AD-Features in Abhängigkeit der Gesamtstrukturfunktionsebene (Microsoft, 2006 e)

3.2.2 Domänenfunktionsebenen

Die Domänenfunktionsebene definiert die domänenweiten Funktionen von Active Directory innerhalb der Netzwerkumgebung. D.h. durch die Domänenfunktionalität wird ausschließlich die Kommunikationsmöglichkeit verschiedener Domänencontroller innerhalb einer Domäne festgelegt. Da in unserem Fall ohnehin eine eigene Domäne erzeugt wird, ist dieser Punkt ausschließlich innerhalb der eigenen Netzwerkumgebung relevant.

Nachfolgend sind die unterstützten Domänencontroller in Abhängigkeit der konfigurierten Domänenfunktionsebene dargestellt:

Domänenfunktionsebene	Unterstützte Domänencontroller
Windows 2000 gemischt (Standard)	Windows NT 4.0 Windows 2000 Windows Server 2003-Produktfamilie
Windows 2000 pur	Windows 2000 Windows Server 2003-Produktfamilie
Windows Server 2003-interim	Windows NT 4.0 Windows Server 2003-Produktfamilie
Windows Server 2003	Windows Server 2003-Produktfamilie

Tabelle 3.3: Domänenfunktionsebenen in Windows Server 2003 (Microsoft, 2006 e)

Die folgende Tabelle stellt die Verfügbarkeit der einzelnen Funktionen in Anhängigkeit der Domänenfunktionsebene dar:

Domänenfunktion	Windows 2000 gemischt	Windows 2000 pur	Windows Server 2003
Tool für die Umbenennung von Domänencontroller	Deaktiviert	Deaktiviert	Aktiviert
Unterschiedliche Speicherorte für Benutzer- und Computerkonten	Deaktiviert	Deaktiviert	Aktiviert

Tabelle 3.4: AD-Features in Abhängigkeit der Domänenfunktionsebene (Microsoft, 2006 e)

Domänenfunktion	Windows 2000 gemischt	Windows 2000 pur	Windows Server 2003
Aktualisieren des Anmeldungszeit-stempels	Deaktiviert	Deaktiviert	Aktiviert
Benutzerkennwort im "InetOrgPerson"-Objekt	Deaktiviert	Deaktiviert	Aktiviert
Universelle Gruppen	Aktiviert für Verteilergruppen Deaktiviert für Sicherheitsgruppen	Aktiviert Ermöglicht Sicherheits- und Verteilergruppen	Aktiviert Ermöglicht Sicherheits- und Verteilergruppen
Gruppenschachtelung	Aktiviert für Verteilergruppen Deaktiviert für Sicherheitsgruppen, außer für lokale Sicherheitsgruppen einer Domäne, die globale Gruppen als Mitglieder haben können	Aktiviert Ermöglicht die vollständige Gruppenschachtelung	Aktiviert Ermöglicht die vollständige Gruppenschachtelung
Konvertieren von Gruppen	Deaktiviert Es sind keine Gruppenkonvertierungen zulässig	Aktiviert Ermöglicht Konvertierungen von Sicherheits- und Verteilergruppen	Aktiviert Ermöglicht Konvertierungen von Sicherheits- und Verteilergruppen
SID-Verlauf	Deaktiviert	Aktiviert Ermöglicht die Migration von Sicherheitsprinzipalen zwischen Domänen	Aktiviert Ermöglicht die Migration von Sicherheitsprinzipalen zwischen Domänen

Tabelle 3.4 Fortsetzung: AD-Features in Abhängigkeit der Domänenfunktionsebene (Microsoft, 2006 e)

3.3 Entscheidung

Anhand eines Vergleichs der Vor- und Nachteile der Möglichkeiten zur Migration der Windows NT 4.0 Domäne und Einführung von Active Directory, muss nun die Entscheidung bezüglich des Active Directory Designs getroffen werden. Diese ist zudem ausschlaggebend für die weitere Planung der Umstellung von Microsoft Windows NT 4.0 auf Microsoft Windows Server 2003.

Nach Darlegung und Diskussion der einzelnen Active Directory Implementierungen wurde aufgrund der in diesem Kapitel behandelten Aspekte und der jeweiligen Vor- und Nachteile der diversen Implementierungen eine Entscheidung für die **Erstellung einer eigenständigen Gesamtstruktur** getroffen.

Die für diese Entscheidung ausschlaggebenden Punkte waren die angestrebte vollkommene Unabhängigkeit in der AD-Struktur und die Tatsache, dass sich der Ressourcenzugriff auf eine Domäne in Deutschland lediglich auf die Authentifizierung für den Internetzugriff beschränkt.

4 Active Directory und DNS / DHCP

Da es sich bei Active Directory um einen Verzeichnisdienst handelt, welcher auf der Verwendung von DNS (Domain Name System) basiert, ist eine einwandfrei funktionierende DNS Umgebung von großer Bedeutung. In früheren Umgebungen wurde ein DNS-Server in einem Netzwerk ausschließlich für die Namensauflösung verwendet. In Active Directory hingegen wird dieses Service zudem auch für das Auffinden von Diensten und Ressourcen in einer Domäne verwendet. Damit diese Aufgabe auch zufriedenstellend erfüllt werden kann, sind bestimmte Anforderungen an ein DNS System zu beachten. Diese Anforderungen werden später in diesem Kapitel genauer erläutert.

Die Funktion des DHCP Servers mit Active Directory wird im Moment nicht als problematisch eingeschätzt, da es sich beim Dynamic Host Configuration Protocol um ein standardisiertes Internet Protokoll handelt und somit die Funktion dieses Dienstes bei den diversen Implementierungen gleich ist.

4.1 Identifikation der bestehenden DNS Struktur

Aufgrund der unzureichenden Funktionen eines Windows NT 4.0 DNS Servers, wurde beim Aufbau des aktuellen Systems ein alternativer DNS Server installiert. Dieser Cisco Network Registrar 5.5.9 DNS Server hat sich bei seinem jahrelangen Einsatz durchaus bewährt und gilt nun auch als strategisches Pro-

dukt der Konzernleitung. Dadurch soll dieser auch nach der Umstellung auf das neue System weiterhin in Verwendung bleiben. Die Fehlertoleranz wurde dabei durch mehrere sekundäre externe DNS Server, welche sich in der Konzernzentrale in Deutschland befinden, realisiert. Nachfolgende Abbildung soll einen Überblick über die bestehende DNS Implementierung geben:

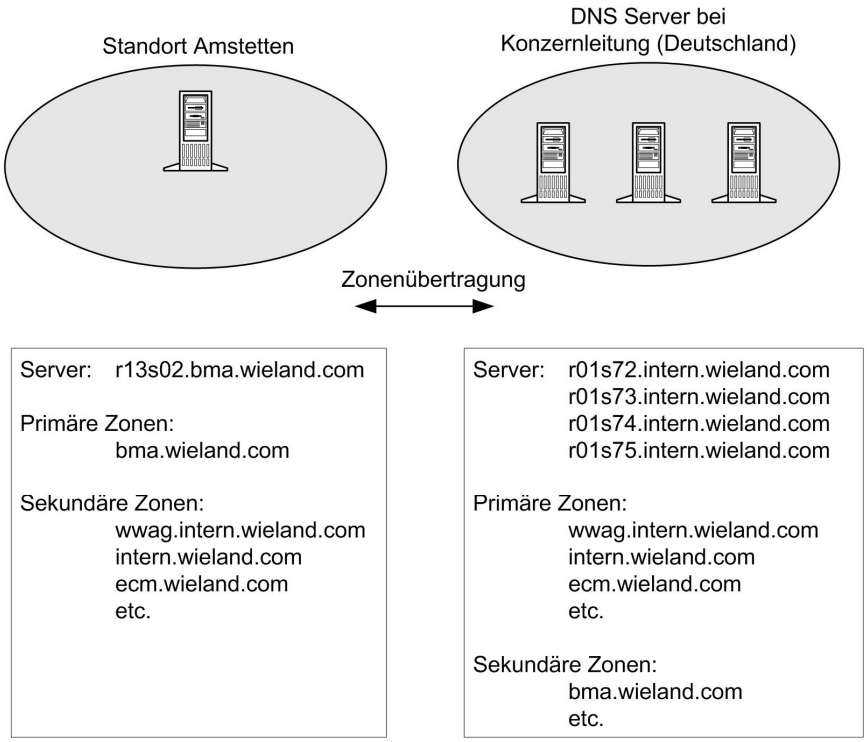

Abbildung 4.1: Bestehende DNS Umgebung

Wie in Abbildung 4.1 dargestellt befindet sich am Standort Amstetten lediglich ein DNS Server r13s02.bma.wieland.com, der als Primary DNS Server für die Zone bma.wieland.com konfiguriert ist. Die Replikation mit den sekundären DNS Servern in Deutschland erfolgt dabei automatisch nach Ablauf des konfigurierten Aktualisierungsintervalls bzw. nach einer Änderung der Zone bma.wieland.com. Den Clients im lokalen Netzwerk werden die IP-Adressen der Server r13s02.bma.wieland.com, r01s75.intern.wieland.com und r01s73.intern.wieland.com als die zu verwendenden DNS Server mittels DHCP zugewiesen.

Für die Migration der Domänen Struktur, muss daher eine Untersuchung betreffend der Möglichkeit der Einführung von Active Directory in die bestehende DNS Struktur durchgeführt werden. Dabei sind die Funktionen und die Unterstützung der Anforderungen des bestehenden DNS Servers Cisco Net-

work Registrar 5.5.9, welche für das Zusammenspiel mit Active Directory benötigt werden, zu untersuchen.

4.2 Anforderungen an DNS in Verbindung mit Active Directory

Wie schon oben erwähnt, benutzen Microsoft Windows Server 2003 und Active Directory den DNS Server nicht ausschließlich zur Namensauflösung, sondern auch um Dienste und Ressourcen (Domänencontroller, Globaler Katalog, etc.) im Netzwerk zu lokalisieren. Dies ist ein neuerer Standard, welcher speziell durch ältere DNS-Server Implementierungen unter Umständen noch nicht unterstützt wird.

Aus diversen Literaturen gehen drei wesentliche Anforderungen an einen DNS Dienst hervor um das Zusammenspiel zwischen Active Directory und dem DNS Server zu ermöglichen. Diese sind die Unterstützung von SRV Records (Service Location Resource Records), die Unterstützung von dynamischen Updates und die Möglichkeit zur Durchführung von Incremental Zone Transfers (IXFR).

Die Unterstützung von SRV Records ist dabei unumgänglich. Mit Hilfe von SRV Records werden in Active Directory ein oder mehrere Server für spezifische Ressourcen bzw. Dienste (wie z.B.: Domänencontroller, der Verzeichnisdienst LDAP, Kerberos, etc.) lokalisiert. Diese müssen auf dem DNS Server eingetragen werden um sicherzustellen, dass Clients die benötigten Dienste auffinden können. Dieses Eintragen kann dabei auf zwei Arten erfolgen, zum einen manuell durch einen Administrator oder aber durch dynamische Updates. Aus diesem Grund wird die Unterstützung der dynamischen Updates auch als nicht unbedingt erforderlich angeführt, wobei jedoch angemerkt ist, dass durch die Unterstützung die Administration wesentlich vereinfacht wird und die Unterstützung somit für die Verwendung von Active Directory empfohlen wird.

Bei Unterstützung von dynamischen Updates werden diese zusätzlichen SRV Resource Records Einträge automatisch während dem Netlogon Prozess des Domänencontrollers auf dem DNS-Server eingetragen.

Auch die Funktion der Incremental Zone Transfer ist dabei kein absolutes Muss, sie birgt allerdings den Vorteil, dass bei Replikation zwischen den DNS Servern nur die geänderten Datensätze übertragen werden, somit die Effizienz dieser Updates gesteigert und die benötigte Bandbreite minimiert wird.

4.3 Integration der bestehenden DNS Struktur

Bei ordnungsgemäßer Unterstützung der oben angeführten Anforderungen, versucht jeder Domänencontroller beim Start des *Netlogon* Dienstes, die erforderlichen Einträge automatisch auf dem DNS Server zu registrieren.

Sollten die erforderlichen Einträge aus irgendeinem Grund während der Installation von Active Directory nicht hinzugefügt werden können oder der DNS Server keine dynamischen Updates akzeptieren, so besteht die Möglichkeit, diese nach der Installation manuell einzutragen oder über ein Skript eintragen zu lassen. Dabei müssen die Einträge, welche bei der Installation automatisch in die Datei *%systemroot%\System32\config\Netlogon.dns* geschrieben werden, auf dem DNS Server eingetragen werden.

Obwohl beide Anforderungen (SRV Records und dynamische Updates) in der von uns verwendetet Version des Cisco Network Registrar 5.5.9 implementiert sind, können diese DNS-Server unter Umständen nicht problemlos mit Windows 2003 benutzt werden. Die Clients benutzen nämlich ein in einem Draft (von Microsoft entwickelt) festgelegtes Protokoll, um die Sicherheit der dynamischen Updates zu gewährleisten.

4.4 Alternative Lösungen

Das angestrebte Ziel, die Weiterverwendung des aktuell im Einsatz befindlichen DNS Servers, hat zur Folge, dass bei Ausfall dieses DNS Servers sämtliche Dienste, welche in der Domäne angeboten werden, für Clients nur über die DNS Server in Deutschland aufgelöst werden können. Grund dafür ist, dass nur ein Server, die für die Lokalisation von Diensten notwendigen SRV Einträge bereitstellt, im lokalen Netzwerk verfügbar ist. Sollte in diesem Fall zusätzlich ein Problem mit der WAN-Verbindung in die Konzernleitung in Deutschland auftreten, haben die Clients keine Möglichkeit, die notwendigen Dienste bzw. Ressourcen zu lokalisieren. Weiters könnte das Zusammenspiel zwischen Cisco Network Registrar und Active Directory, wie oben beschrieben, ein zusätzliches Problem darstellen. Deshalb sollte eine Lösung bereitgestellt werden, womit diese Probleme vermieden werden können und zusätzliche Redundanz im lokalen Netzwerk geschaffen werden.

4.4.1 Variante 1

Eine mögliche Variante des zukünftigen Systems könnte die Migration der Umgebung unter der Verwendung der bisherigen DNS-Zone bma.wieland.com, wie in nachfolgender Abbildung darstellen.

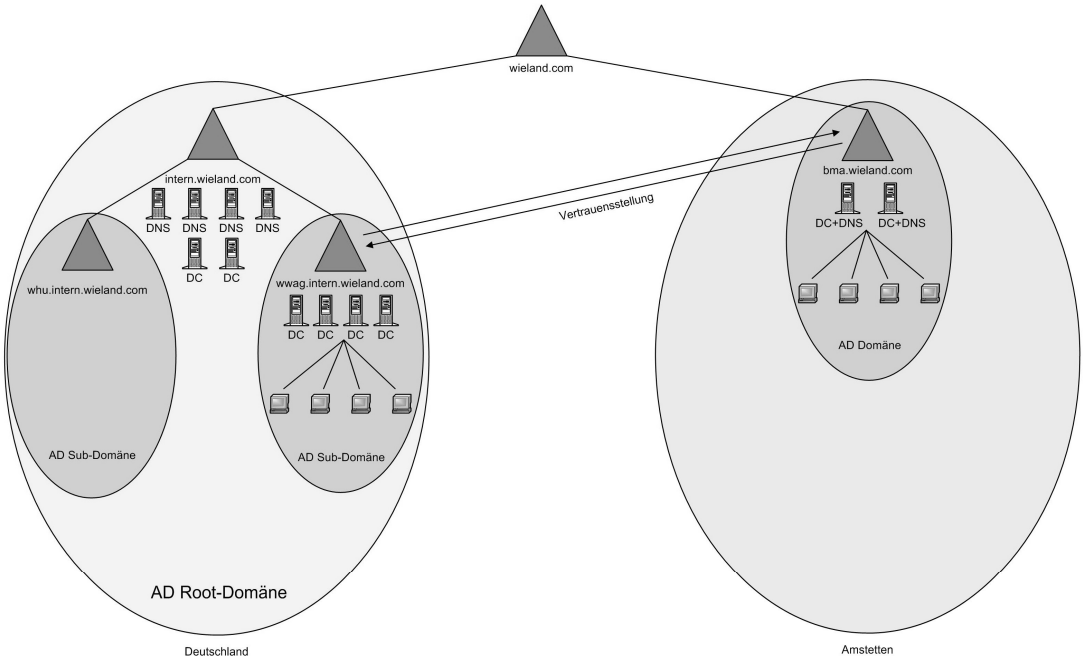

Abbildung 4.2: Variante 1 zukünftige Struktur

Dies ist aber nur sinnvoll, wenn mit dieser Domäne keine öffentlichen Ressourcen wie z.B.: Internetseiten, Shops oder Remotezugänge angesprochen werden. Andernfalls würde man interne und öffentliche Ressourcen in eine Zone bringen, wodurch eine viel komplexere und vor allem verwirrendere DNS-Implementierung erfolgen müsste. Falls keine öffentlichen Ressourcen erreicht werden müssen, ist diese Lösung durchaus umsetzbar.

Bei dieser Lösung müsste noch eine Entscheidung bezüglich der eingesetzten DNS Server Software erfolgen. Für den einwandfreien Betrieb von Active Directory scheint der Einsatz von Microsoft DNS Server am sinnvollsten (s. Punkt 4.4.3). Es ist aber durchaus die Weiterverwendung des im Moment betriebenen Cisco Network Registrar DNS Server denkbar.

4.4.2 Variante 2

Um der unzulänglichen Fehlertoleranz entgegenzuwirken, sollte ein Konzept für eine DNS Struktur mit mehreren DNS-Servern erstellt werden. Dabei ist es sinnvoll die auf Windows Server 2003 migrierten Domänencontroller zusätzlich als DNS Server zu installieren.

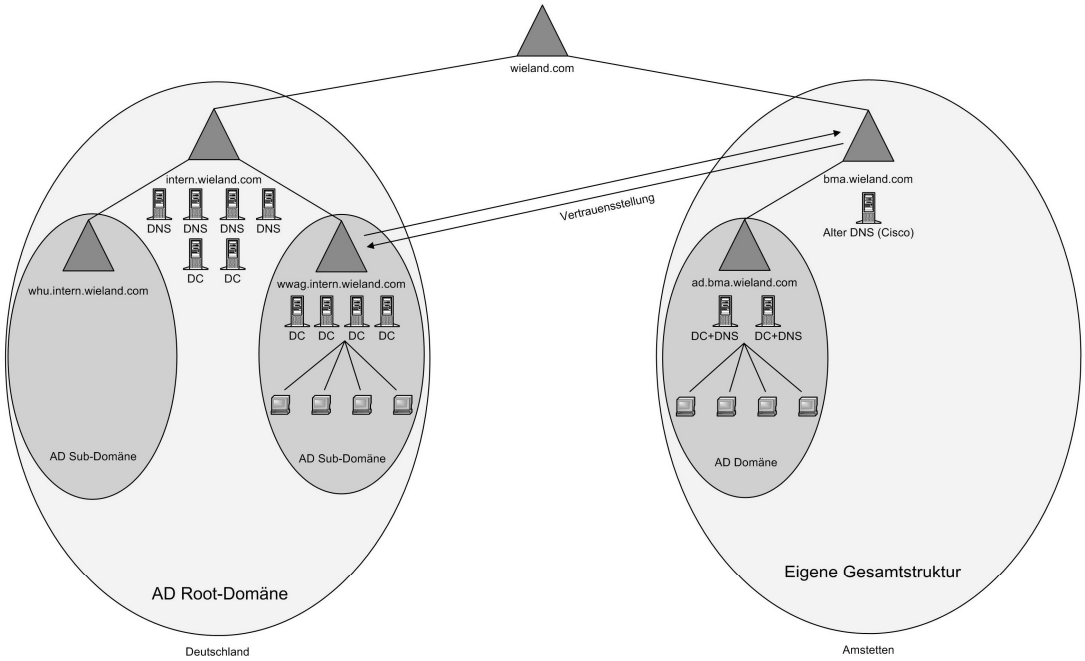

Abbildung 4.3: Variante 2 der zukünftigen Struktur

Dies birgt den Vorteil, dass sämtliche Registrierungen in Verbindung mit Active Directory direkt von den Domänencontrollern verarbeitet werden können und somit keine Probleme bezüglich der Registrierung von SRV Records am Cisco Network Registrar DNS Server auftreten können. Die Verwendung eines DNS Servers von Microsoft bietet zudem einen wesentlichen Vorteil, auf welchen in Punkt 4.4.3 näher eingegangen wird.

Um jedoch sämtliche außerhalb der Domäne befindlichen Ressourcen zu lokalisieren, ist die Weiterleitung von Anfragen, welche die neuen DNS Server nicht beantworten können, an den bislang einzigen DNS Server zu konfigurieren. Somit kann das Active Directory auch bei einem Ausfall des Cisco Network Registrar DNS Server die korrekte Funktion aufrechterhalten.

Bei dieser Lösung wirft sich natürlich die Frage auf, inwiefern die Weiterverwendung des Cisco Network Registrar DNS Servers noch sinnvoll ist, da dieser

somit der dritte DNS Server in der Domäne ist und dessen Dienste natürlich von den beiden anderen DNS Servern, nach dementsprechender Konfiguration übernommen werden könnten. Natürlich kann durch die Argumentation, dass es sich bei diesem Cisco Network Registrar DNS Server um ein strategisches Produkt der Konzernleitung handelt, die weitere Verwendung begründet werden. Außerdem schafft man durch Weiterverwendung der bestehenden DNS Struktur eine bessere Skalierbarkeit. Denn durch den Fortbestand der Zone bma.wieland.com könnte eine eventuelle zukünftige Bereitstellung von öffentlichen Ressourcen ohne Probleme erfolgen, da man in der Lage wäre öffentliche von internen Ressourcen zu trennen.

Eine weitere Möglichkeit, das Problem der mangelnden Fehlertoleranz zu beseitigen, ist eine Installation eines zusätzlichen Cisco Network Registrar DNS Servers durchzuführen. Dies setzt natürlich voraus, dass sich dieser während der Testimplementation in Kombination mit den SRV Ressourcen Einträgen und den dynamischen Updates bewährt und jegliche Beeinträchtigungen des einwandfreien Betriebs ausgeschlossen werden können.

Um die Vertrauensstellung, wie in Abbildung 4.3 dargestellt, erstellen zu können, muss für eine korrekte Auflösung der beiden DNS Zonen ad.bma.wieland.com und wwag.intern.wieland.com gesorgt werden.

4.4.3 Microsoft Integrated DNS Server

Ein weiterer sehr wichtiger Aspekt, der für die Verwendung eines DNS Servers von Microsoft spricht ist, dass Microsoft ein eigenes Konzept für die Integration von DNS Servern bereitstellt – die Funktion des Active Directory-Integrated DNS. Dabei gelten im Gegensatz zu einem herkömmlichen DNS System, bei welchen es immer einen primären und einen oder mehrere sekundäre DNS Server gibt, alle DNS Server als gleichberechtigt. D.h., dass sämtliche Active Directory-Integrated DNS Server eine *read/write* Kopie der DNS Datenbank enthalten und somit jeder dieser Server zu Änderungen an der Datenbank berechtigt ist.

Im Gegensatz dazu besitzt bei herkömmlichen DNS Systemen nur der primäre DNS Server eine solche Kopie und alle sekundären Server nur eine *read* Kopie. Das hat zur Folge, dass es bei Ausfall des primären DNS Servers zu sehr langen Bootvorgängen (Anmeldezeiten) kommen kann, da die Clients den primären DNS Server nicht auffinden können und die sekundären Server keine Updates akzeptieren.

4.5 Entscheidung

Auch hier muss eine Entscheidung bezüglich der geplanten Implementierung des zukünftigen DNS Dienstes erfolgen. Nach Erarbeitung der verschiedenen Implementierungsmöglichkeiten ist hierbei eine Entscheidung für die **Beibehaltung der derzeitigen DNS Infrastruktur** getroffen worden. D.h., dass der momentan in Verwendung befindliche DNS Server Cisco Network Registrar weiterhin als primärer DNS Server für die Zone bma.wieland.com im Einsatz bleiben soll. Da aber auch die notwendige Fehlertoleranz innerhalb der lokalen Netzwerkinfrastruktur bereitgestellt werden soll, werden auf den Domänencontrollern zusätzliche DNS Server installiert.

Wie in den vorangegangen Punkten festgehalten wurde, handelt es sich bei dieser Implementierung nicht um die technisch sinnvollste Lösung. Aufgrund der Tatsache, dass seitens der Konzernleitung jedoch keine Microsoft DNS Server im Einsatz sind, wurde hier eine Kompromisslösung mit der IT Abteilung der Konzernleitung angestrebt, welche die Aufrechterhaltung des Betriebs der bestehenden DNS Lösung bevorzugt.

5 Auswahl eines Migrations-Pfades

Da für die Migration mehrere mögliche Szenarien existieren, muss zuvor die Wahl des Migrations-Pfades getroffen werden. Dabei ist es notwendig die erwarteten Verbesserungen durch eine Migration zu erkennen. Für die letztendliche Wahl eines Migrations-Pfades ist es weiters wichtig, Unternehmens- und Migrationsziele zu definieren. Diese sollen sowohl die Erwartungen und Anforderungen an das zukünftige System, als auch die organisatorischen Abläufe im Unternehmen möglichst deutlich darstellen. Durch einen abschließenden Vergleich dieser Ziele mit den Vor- und Nachteilen der einzelnen Migrations-Pfade, muss letztendlich eine Entscheidung bezüglich des bevorzugten Migrations-Pfades getroffen werden.

5.1 Vorteile der Migration

Für die Entscheidung ob eine Migration durchgeführt werden soll, ist auch eine Erkenntnis bezüglich der dadurch entstehenden Vorteile nötig. Die Analyse der Vorteile kann vor allem zur Argumentation gegenüber dem Management eines Unternehmens verwendet werden, um diese von der Notwendigkeit dieser Umstellung zu überzeugen.

Nachfolgende Punkte sollen die wesentlichsten Vorteile einer Umstellung der Domäne von Microsoft Windows NT 4.0 auf Windows Server 2003 Standard Edition klarstellen:

- Effizientere zentrale Administration

  Dank einheitlicher Verwaltungswerkzeuge wie Microsoft Management Console (MMC) und dem Einsatz von Richtlinien und Automatisierung von Tasks können Benutzer und Ressourcen leichter verwaltet werden. Die Verbesserung der Administration ermöglicht somit eine weniger zeitintensive und kostensparende Verwaltung der Domäne.

- Change & Configuration Management

  Dieser Punkt umfasst die verbesserten Möglichkeiten eines Administrators auf Änderungen in der Organisation des Unternehmens zu reagieren wie zum Beispiel Änderungen von Domänen-Namen.

- Hohe Sicherheit, Zuverlässigkeit, Stabilität und Vielseitigkeit

  Neue Sicherheitsmechanismen und Features des neuen Betriebssystems bringen wesentliche Vorteile in der Systemleistung und bieten zu dem verbesserte Skalierbarkeit und Verfügbarkeit mit geringeren Ausfallzeiten des neuen Systems. Auch die Unterstützung von aktuellen Prozessor- und Netzwerktechnologien ist hierbei wesentlich.

- Unterstützung für Software – Ablösung von NT 4.0

  Da einige Support-Kategorien für das alte Betriebssystem Windows NT 4.0 Server bereits ausgelaufen sind und auch der Online-Support mit 31.12.2006 ausläuft, stellt der Weiterbetrieb dieses Systems ein wesentliches Sicherheitsrisiko dar.

- Nutzung aller Vorteile eines zentralen, fehlertoleranten, verteilten Authentisierungs- und Verzeichnisdienstes (Active Directory)

- Bereit für das Internet

  Integrierte Webdienste bieten die Möglichkeit, Internet- oder Intranet-Anwendungen sofort auf Windows Server 2003 zu nutzen.

- Integrierte PKI (Public Key Infrastructure) Unterstützung

  Bietet Unternehmen die Möglichkeit eine eigene PKI für das Management und die Verteilung von Zertifikaten zu implementieren. Auch die Unterstützung der verbesserten Authentifizierung (Kerberos) und die Einsatzmöglichkeit von IPSec sind wesentlicher Bestandteil von Microsoft Windows Server 2003.

- Command-Line Management

  Die gesamte Konfiguration kann auch mittels eines Kommandozeilenprogramms erfolgen und bietet somit die Verbesserung in der Remote Verwaltung, im speziellen wenn diese über Leitungen mit geringer Bandbreite geschieht.

5.2 Unternehmensziele der Migration

Jedoch sind nicht nur die Vorteile der Migration für die Entscheidung zur Durchführung relevant. Auch eine Analyse der Unternehmensziele und der Erwartungen an das neue System stellen eine wesentliche Grundlage für den Startschuss der Umstellung dar.

Nachfolgende Punkte stellen die Unternehmensziele, welche bei der Migration der Domäne zu beachten und umzusetzen sind, dar:

- Beibehaltung der Struktur

  Da die derzeitige Struktur nur aus einer einzigen Windows NT 4.0 Domäne besteht, ist eine weitere Vereinfachung der Organisation der Domäne kaum möglich. Aus diesem Grund wird die Beibehaltung der aktuellen Struktur angestrebt. Ein weiteres Ziel ist, da es sich bei der vorhandenen Domäne um eine untergeordnete Domäne der Konzernzentrale handelt, dass sämtliche Vertrauensstellungen zu der

übergeordneten Domäne erhalten bleiben bzw. neu erzeugt werden und die seitens der Konzernleitung eventuelle notwendig werdenden Änderungen minimiert werden.

- Zentrale Administration

  Da die Domäne nur einen Standort versorgt und sämtliche Komponenten lokal installiert sind, wird auch nach Umstellung der Domäne die Administration zentral erfolgen.

- Reduzierung der Ausfallzeit

  Aufgrund der Arbeitsprozesse im Unternehmen, welche nur eine geringe Beeinträchtigung der Verfügbarkeit von Diensten und Anwendungen erlauben, muss die Umstellung schnellstmöglich und mit geringst möglichen Ausfallzeiten dieser Dienste und Anwendungen erfolgen.

- Einsatz vorhandener Komponenten

  Durch die begrenzten finanziellen Mittel, soll die Umstellung, soweit als möglich, unter Benutzung der bereits vorhandenen Komponenten erfolgen. Die Kosten für Neuanschaffungen sollen so gering wie möglich gehalten werden.

- Umsetzung von Unternehmensvorgaben

  Da es seitens der Konzernleitung diverse Vorgaben wie z.B.: die Verwendung eines alternativen DHCP und DNS Servers gibt, soll die Umstellung unter Berücksichtigung dieser Punkte erfolgen. Für den Fall, dass sich diese Vorgaben nicht ohne größere Schwierigkeiten erfüllen lassen, muss eine alternative Lösung entwickelt werden.

- Rollback Möglichkeit

  Bei unvorhergesehenen eventuell auftretenden Problemen, für die innerhalb einer kurzen Zeitspanne keine entsprechende Lösung bereitgestellt werden kann, muss die Möglichkeit bestehen, das ursprüngliche System wiederherzustellen.

5.3 Möglichkeiten der Migration

Die Migration einer Windows NT 4.0 Domäne in eine Windows Server 2003 Domäne kann auf unterschiedliche Arten erfolgen. Dabei sind die Vor- und Nachteile der einzelnen Wege abzuwägen und mit den Anforderungen an das zukünftige System und die Migration zu vergleichen. Die Analyse der verschieden Wege stellt eine weitere Grundlage für die Wahl jenes Migrationspfades dar, wodurch die festgelegten Unternehmensziele am zielführendsten umgesetzt werden können.

5.3.1 Domain Upgrade

Beim Domain Upgrade (auch In-Place Upgrade) werden die bestehenden Domänencontroller mittels Update auf das neue Betriebssystem hochgerüstet. Die Methode des Domain Upgrade ist besonders für Unternehmen interessant, deren Infrastruktur als eher klein bezeichnet werden kann, und welche mit der derzeitigen Struktur ihrer Domäne zufrieden sind. Bei diesem Verfahren ist keine Veränderung der Struktur möglich, dies sollte bestenfalls noch vor der Umstellung erfolgen oder nach Abschluss des Upgrades (s. Punkt 5.3.3). Neben der schnellst möglichen und einfachsten Umsetzung birgt diese Methode einer Migration das geringste Risiko.

5.3.2 Domain Restructure

Bei dieser Methode erfolgt eine Umstrukturierung der Struktur als Ganzes oder zumindest in Teilen und ist somit für Unternehmen interessant, welche eine komplette Umstellung des Systems benötigen um ihre Unternehmens- bzw. Migrationsziele zu erreichen. Da die Organisationseinheiten unter Windows NT 4.0 die Domänen waren und diese aufgrund der beschränkten Größe der SAM Datenbank eingegrenzt werden mussten, ist in vielen Unternehmen über die Jahre eine „gewachsene" Struktur entstanden, die mittlerweile nur sehr schwer überschaubar und administrierbar ist. Deshalb stellt das Domain Restructure für diese Gegebenheiten die bestmögliche Migrationslösung dar, da dadurch eine Konsolidierung der vorhandenen Struktur möglich ist um damit eine vereinfachte und vereinheitlichte Administration zu schaffen. Das Domain Restructure lässt sich dabei in weitere Unterpunkte unterscheiden.

5.3.2.1 Post-Upgrade

Dies ist eine andere Bezeichnung für die Methode Domain Restructure und anschließendes Domain Upgrade worauf im Punkt 5.3.3 näher eingegangen wird.

5.3.2.2 Anstatt des Upgrades

Falls die Infrastruktur eines Unternehmens nicht mehr der wirtschaftlichen Verfolgung der Unternehmensziele dient oder das Risiko eines Upgrade aufgrund der geforderten Stabilität des Betriebes zu hoch erscheint, können diese Unternehmen einen kompletten Neuaufbau ihrer Domänen Struktur anstreben. Für diese Unternehmen ist es somit einfacher eine ideale Windows Server 2003 Struktur zu schaffen und anschließend sämtliche Objekte wie User, Computer, etc. in die neue Struktur zu migrieren.

5.3.2.3 Post-Migration

Dieser Punkt beschreibt die Umstrukturierung einer bereits bestehenden, ausschließlich mittels Windows Server 2003 aufgebauten Umgebung, um diese an Änderungen der Organisation eines Unternehmens anzupassen.

5.3.3 Domain Restructure und anschließendes Domain Upgrade

Dabei erfolgt im Wesentlichen ein Domain Upgrade mit anschließender Restrukturierung. Dieser Weg ist besonders interessant für Unternehmen mit größeren Domänen Strukturen und dem Ziel, diese in einer neuen zusammengefassten Organisation zu verwalten.

5.4 Entscheidungspunkte für die Wahl des Migrations-Pfades

Wie schon oben erwähnt gibt es für jeden dieser Migrations-Pfade Aspekte die für bzw. gegen die Wahl der jeweiligen Art der Migration sprechen. Diese werden nun nachfolgend angeführt (vgl. Microsoft, 2000):

5.4.1 Gründe für Domänen Upgrade

- Die gegenwärtige Domänen Struktur entspricht den Zielen der Migration und man kann einen Zwei-Phasen-Plan, welcher eine anschließende Restrukturierung beinhaltet, anstreben.
- Die Migration kann ohne Beeinträchtigung der Produktionsumgebung durchführt werden.
- Die existierende Ausstattung entspricht den Anforderungen der Migrationsziele.
- Limitierung der kurzfristigen Ressourcen – begrenzte Möglichkeit zur Anschaffung neuer Komponenten
- Eine Änderung der Infrastruktur bringt zu große Änderungen in der Organisation mit sich.
- Die Organisation der administrativen Aufgabe soll erhalten bleiben.
- Die Wiederherstellung des Ausgangzustandes soll möglich sein.
- Aufgrund der Inkompatibilität einer Applikation wird eine Domänen Restrukturierung verhindert.
- Es wird eine schnelle Migrationslösung benötigt.

5.4.2 Gründe gegen Domänen Upgrade

- Es wurde eine unwirtschaftliche oder veraltete Domänen Struktur erkannt und diese soll nicht in das neue System übernommen werden.
- Wenn festgestellt wird, dass die Umstellung keine Reduzierung der Administrationskosten bewirkt.
- Es wird erkannt, dass durch die Umstellung keine Reduzierung erfolgt.
- Falls Beeinträchtigungen durch die Umstellung zu erwarten sind.

5.4.3 Gründe für Domänen Restrukturierung

- Die gegenwärtige Domänen Struktur entspricht den Zielen der Migration und man kann einen Zwei-Phasen-Plan, welcher ein vorheriges Upgrade beinhaltet, anstreben.
- Die aktuelle Domänen Struktur entspricht nicht den Anforderungen des Unternehmens.
- Es sind Beeinträchtigungen durch ein Domain Upgrade zu erwarten.
- Eine Reduzierung der längerfristigen Hardware- und Administrationskosten wird angestrebt.
- Unwirtschaftliche und veraltete Domänen Strukturen sollen beseitigt werden.
- Die weitere Verwendung von alter Hardware ist nicht geplant.

5.4.4 Gründe gegen Domänen Restrukturierung

- Die existierende Infrastruktur entspricht den Anforderungen des Unternehmens
- Die Domäne muss in Mixed Mode betrieben werden.
- Neue Infrastruktur benötigt neue IT Funktionen welche noch nicht definiert sind
- Die möglicherweise kurzfristige Erhöhung der Hardware Kosten

5.4.5 Gründe für Domänen Upgrade und anschließende Restrukturierung

- Unwirtschaftliche und veraltete Domänen Strukturen sollen beseitigt werden.
- Eine Wiederherstellung des Ausgangzustandes soll möglich sein.
- Reduzierung der kurzfristigen Hardware- und Administrationskosten
- Die Durchführung soll außerhalb der Produktionsumgebung stattfinden

- Abteilungsorientierte LANs sollen sich zu einer zentralisierten Infrastruktur entwickeln

5.4.6 Gründe gegen Domänen Upgrade und anschließende Restrukturierung

- Die zweiphasige Methode braucht länger in der Planung.
- Die zweiphasige Methode braucht länger in der Umsetzung.

5.5 Entscheidung

Anhand eines Vergleiches der Vor- und Nachteile jeder Migrationslösung mit den Erwartungen bzw. Anforderung der Migration selbst und des anschließenden Betriebs der neuen Umgebung muss nun die Entscheidung bezüglich der Methode der Migration getroffen werden. Diese ist zudem ausschlaggebend für die weitere Planung der Umstellung von Microsoft Windows NT 4.0 auf Microsoft Windows Server 2003.

Nach Darlegung und Diskussion der einzelnen Migrationsverfahren, wurde aufgrund der in diesem Kapitel angeführten Unternehmens- und Migrationsziele und der jeweiligen Vor- und Nachteile der diversen Migrationsmöglichkeiten klar, dass die für die Migration der Windows NT 4.0 Domäne der Firma Buntmetall Amstetten GmbH eine Lösung entworfen werden soll, welche so wenige Änderungen der bestehenden Struktur mit sich bringt, wie nur irgendwie möglich. Weiters wurde festgelegt, dass eine möglichst rasche Migrationslösung zu bevorzugen ist. Aus diesen Gründen wurde die Entscheidung zugunsten eines **Domänen Upgrade** getroffen. Diese Entscheidung wurde zudem auch noch durch den Aspekt, dass bei dieser Methode eine relativ einfache Wiederherstellungsmöglichkeit des Ausgangszustandes existiert, bestärkt.

6 Planung der Migration

Um auf eventuelle Probleme während der Migration schnellst möglich und richtig reagieren zu können, ist eine detaillierte Planung der Reihenfolge der durchzuführenden Schritte unabdingbar. Aber auch zur Messung des Erfolgs bzw. des Fortschritts der Migration kann die vorangegangene Migrationsplanung herangezogen werden. Für eine genaue Planung und Vorbereitung auf die Umstellung muss eine Testumgebung in welcher die einzelnen Schritte erprobt werden können aufgebaut werden.

Grundsätzlich kann eine Einteilung der Migration in drei Phasen erfolgen, die Vorbereitungs-, die eigentliche Migrations- und die Nachbearbeitungsphase.

6.1 Ermittlung der Upgrade Möglichkeit

Da die Möglichkeit eines Upgrades von einem Betriebssystem auf ein anderes immer von der installierten Version abhängig ist, müssen zuvor die unterstützten Upgrade-Pfade untersucht werden. Nachfolgende Tabelle soll einen Überblick über die unterstützten Upgrade-Pfade lt. Microsoft geben:

Plattform	Upgrade auf Windows Server 2003, Standard Server	Upgrade auf Windows Server 2003, Enterprise Server	Upgrade auf Windows .NET Datacenter Server
Windows NT 4.0 Server - Standard	•	•	
Windows NT 4.0 Server - Enterprise		•	
Windows 2000 Server	•	•	
Windows 2000 Advanced Server		•	
Windows 2000 Datacenter Server			•

Tabelle 6.1: Unterstützte Upgrade-Pfade auf Windows Server 2003 (Microsoft, 2006 c)

Da bei der Firma Buntmetall Amstetten GmbH auf den Domänencontrollern lediglich Microsoft Windows NT 4.0 Standard Server eingesetzt wird und eine Migration auf Microsoft Windows Server 2003 Standard Edition erfolgen soll, stellt diese Migration einen vom Betriebssystem unterstützten Upgrade-Pfad dar. Es ist somit möglich das Betriebssystem direkt auf den „alten" Domänencontrollern zu installieren, sofern deren Hardware dies unterstützt.

6.2 Wiederherstellungsplan

Für den Fall, dass das Upgrade des Betriebssystems nicht wie erwartet verläuft und in der Notwendigkeit einer Wiederherstellung resultiert, muss ein geeigneter Wiederherstellungsplan entworfen werden. Zu diesem Zweck ist es sinnvoll einen vorhandenen BDC vollständig zu synchronisieren, diesen dann vom Netz zu nehmen und als Rollback Server für eine eventuelle Wiederherstellung der Domäne in den ursprünglichen Zustand aufzubewahren. Zusätzlich zu dieser Maßnahme sollte auch eine Sicherung auf ein Speichermedium erfolgen um somit auf die Eventualität, dass dieser Rollback Server die Funktion verweigert, reagieren zu können.

Grundsätzlich gibt es zwei Möglichkeiten um das System wieder in den ursprünglichen Zustand zu versetzen, wobei die nachfolgende als die bessere Methode beschrieben wird:

- Trennung aller Windows Server 2003 Domänencontroller (entweder durch Ausschalten oder Abhängen vom Netzwerk)

- Heraufstufung eines Windows NT 4.0 BDCs zu einem PDC
- Synchronisation aller Domänencontroller

Da es unter Umständen zu einer Beschädigung der SAM-Datenbanken auf allen Domänencontrollern kommen kann, gibt es eine zweite Möglichkeit zur Wiederherstellung des ursprünglichen Zustands:

- Trennung aller Domänencontroller, sowohl Windows Server 2003 als auch Windows NT 4.0 Server Domänencontroller (entweder durch ausschalten oder Abhängen vom Netzwerk)
- Heraufstufung des Rollback Servers zu einem PDC und diesen anschließend in das Netz hängen
- Neuinstallation eines oder mehrerer BDCs
- Replikation zwischen allen Domänencontroller

Ein wesentlicher Schritt bei beiden Methoden ist, dass sämtliche Windows 2003 Domänencontroller offline genommen werden, da ansonsten das Hochstufen eines BDC zum PDC nicht möglich ist.

6.3 Definition der Reihenfolge für das Upgrade von Domänen

Da die Infrastruktur der Firma Buntmetall Amstetten GmbH lediglich eine Kontendomäne beinhaltet, müssen keine weiteren Überlegungen bezüglich der Reihenfolge des Upgrades mehrerer Domänen angestellt werden, wie dies zum Beispiel in größeren Organisationen mit mehreren Domänen der Fall wäre.

6.4 Definition der Reihenfolge für das Upgrade der einzelnen Domänencontroller

Nach den Überlegungen bezüglich der Reihenfolge des Upgrades der einzelnen Domänen, muss nun eine Reihenfolge, in welcher die Domänencontroller aktualisiert werden, definiert werden. Da bei einer Migration immer der PDC zuerst aktualisiert werden muss, ist dafür zu sorgen, dass dieser die Hardwareanforderungen unterstützt. Sollte dies nicht der Fall sein, so kann auch ein vorhandener BDC, welcher die benötigte Hardware besitzt, zum PDC heraufgestuft werden. Tritt der Fall ein, dass keiner der Server ein Upgrade auf Windows Server 2003 unterstützt, so muss ein neuer BDC mit Windows NT 4.0 installiert und zum PDC heraufgestuft werden.

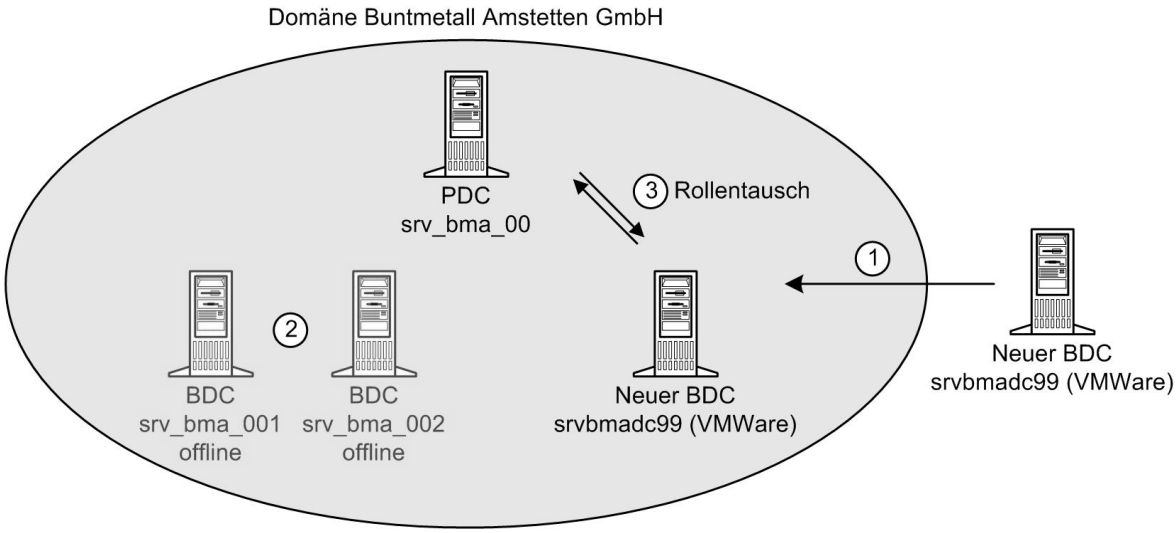

Abbildung 6.1: Ablauf der Migration (Teil 1)

Auch bei der Migration der Domäne der Firma Buntmetall Amstetten GmbH wird diese Methode zur Anwendung kommen, da die vorhandenen BDCs für ein Upgrade auf Microsoft Windows Server 2003 nicht mehr geeignet sind und somit nach der Migration außer Betrieb genommen werden. Somit wird auch hier zuerst ein Server mit geeigneter Hardware als BDC der Windows NT 4.0 Domäne hinzugefügt. Nach der Heraufstufung dieser Server zum PDC kann die Migration auf diesem Server durchgeführt werden.

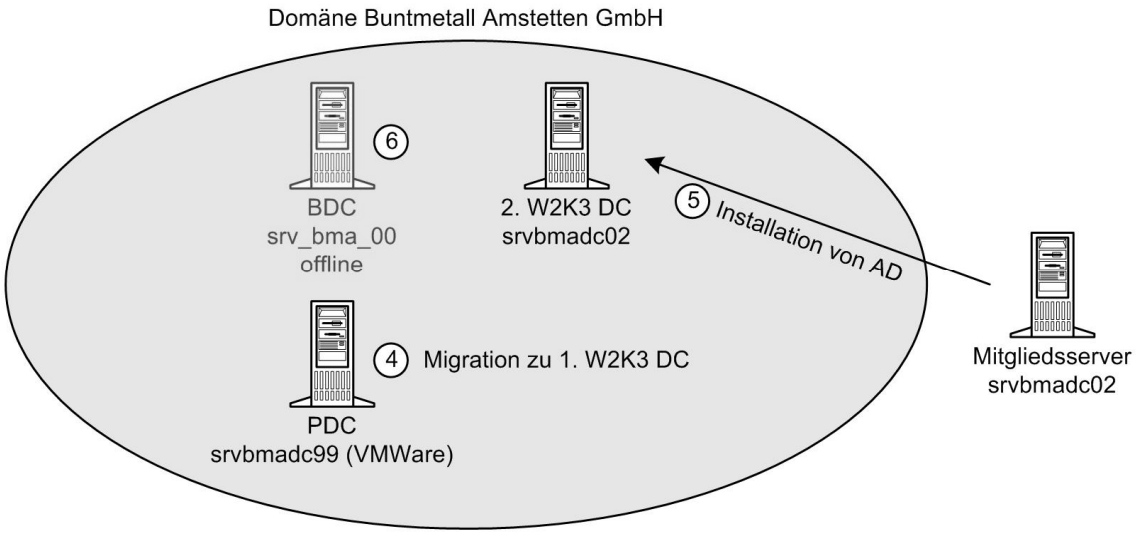

Abbildung 6.2: Ablauf der Migration (Teil 2)

Anschließend wird ein weiterer neuer Server als zusätzlicher Domänencontroller für die neue Windows 2003 Domäne bma.wieland.com installiert. Da von den bestehenden Domänencontrollern nur ein Einziger ein Upgrade unterstützt und der zuerst migrierte Server als virtueller Server (VMWare) installiert wurde, wird dieser als zusätzlicher Domänencontroller installiert werden. Danach kann der zuerst migrierte Server wieder von der Domäne sauber entfernt werden, also durch Entfernen der Funktion als Domänencontroller.

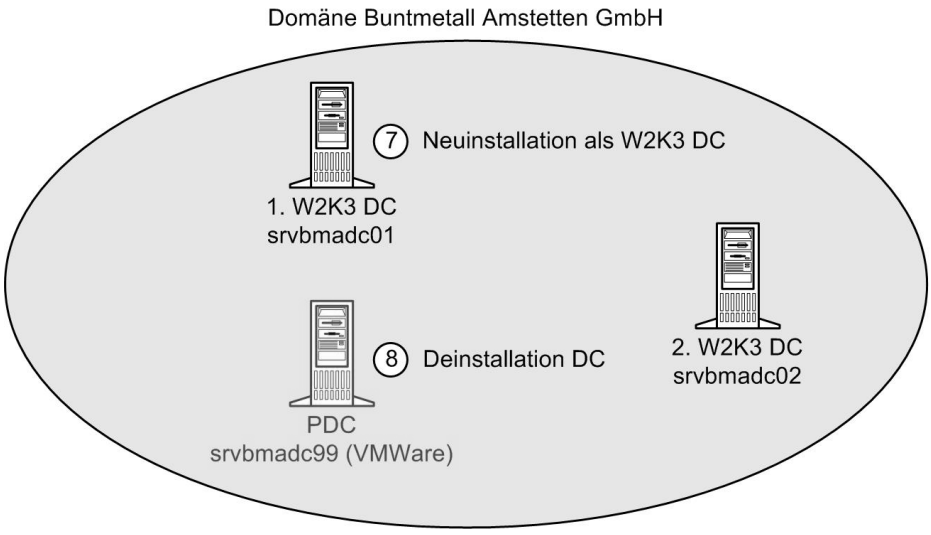

Abbildung 6.3: Ablauf der Migration (Teil 3)

6.5 Definition des Zeitpunkts zum Heraufstufen von Domänen- und Gesamtstrukturfunktionalität

Um sämtliche Funktionen und Vorteile des neuen Betriebssystems zu aktivieren und auch nutzen zu können, muss eine Heraufstufung der Domänen- und Gesamtstrukturfunktionsebene erfolgen. Dieser Schritt ist allerdings erst möglich, wenn sich keine Domänencontroller unter Windows NT 4.0 oder Windows 2000 in der Domäne befinden, da diese nach Heraufstufung der Funktionsebene nicht mehr funktionieren würden. Zudem sollte auch sichergestellt werden, dass diese Betriebssysteme auch in Zukunft nicht für diverse Funktionen zur Domäne hinzugefügt werden müssen.

Da dieser Vorgang irreversibel ist, sollte der Zeitpunkt dafür genauestens überlegt werden und nicht vor einem über einen gewissen Zeitraum definierten Probebetrieb der neuen Domäne erfolgen. Dadurch wird sichergestellt, dass ein Rückstieg auf die Windows NT 4.0 Domäne nicht mehr notwendig ist.

Da in der Domäne bma.wieland.com keine Windows NT 4.0 bzw. Windows 2000 Domänencontroller mehr eingesetzt werden sollen, und auch in der Gesamtstruktur keine Domänen mit diesen Servertypen im Einsatz sind, ist ein Heraufstufen der Domänen- und Gesamtstruktur- Funktionsebene möglich. Dieser Schritt wird aber erst nach einem mindestens 4-wöchigen Probebetrieb erfolgen.

Die genauen Funktionen und unterstützten Betriebssysteme der einzelnen Funktionsebenen wurden bereits in Punkt 3.2 behandelt.

6.6 Festlegung der Nachbearbeitungsaufgaben

Nach Upgrade der Domänencontroller sollten nachfolgend angeführte Punkte durchgeführt werden, um die grundlegende Konfiguration der Domänencontroller zu überprüfen und dessen fehlerfreie Funktion zu garantieren.

6.6.1 Überprüfung des Event-Logs

Um auf eventuelle Fehler, welche während des Upgrades bzw. beim ersten Start des neu aktualisierten Domänencontrollers aufgetreten sind, zu reagieren, muss eine Überprüfung des Ereignis-Protokolls stattfinden.

6.6.2 Überprüfung der Dienste in der Computerverwaltung

Dienste welche für den Betrieb der Domäne notwendig sind, sollten dahingehend überprüft werden, dass diese auch automatisch beim Systemstart geladen werden, ohne dass ein Eingreifen eines Administrators notwendig wird.

6.6.3 Optimierung der Speichereinstellungen

Um sicherzustellen, dass der Domänencontroller die Anforderungen für die ihm zugewiesene Rolle erfüllt, soll eine Überprüfung der Einstellungen der Systemleistung erfolgen.

6.6.4 Überprüfung der TCP/IP Netzwerkeinstellungen

Letztendlich hat eine Überprüfung der angewandten Netzwerkkonfiguration wie IP-Adresse, verwendete DNS und WINS Server und das Standard-Gateway zu erfolgen. Diese kann mit Hilfe des Befehls **ipconfig/all** über die Kommandozeile verifiziert werden.

7 Update auf Windows Server 2003 – Active Directory

In diesem Kapitel sollen die einzelnen Schritte des Upgrades der Windows NT 4.0 Domäne in eine Windows Server 2003 Domäne behandelt werden. Dieser Leitfaden wurde anhand der Unternehmensstruktur der Firma Buntmetall Amstetten GmbH erstellt und muss für andere Domänen, den Bedürfnissen und Gegebenheiten der jeweiligen Domänen angepasst werden.

7.1 Backup des PDC und eines BDC

Wie schon in Punkt 6.2 erwähnt, müssen gewisse Schritte zur Anwendung kommen, um bei Auftreten von Problemen entsprechende Maßnahmen setzen zu können. Die hierfür notwendigen Schritte umfassen das Erstellen eines Backups für den PDC und einen BDC. In weiterer Folge wird ein BDC offline genommen und als Rollback-Server aufbewahrt. Dies ermöglicht die rasche

Möglichkeit des Rückstiegs auf die Windows NT 4.0 Domäne. Für nähere Informationen zum Rückstieg auf das ursprüngliche System s. Punkt 6.2.

7.2 Installation eines Windows NT 4.0 BDC

Da bei der Firma Buntmetall Amstetten GmbH die Migration des Primary Domänencontrollers auf einem virtuellen Server durchgeführt wird, muss zunächst ein Windows NT 4.0 Server als Backup-Domänencontroller auf dem VMWare Server installiert werden.

Weiters muss der LAN Manager Replikationsdienst dieses neuen BDCs so konfiguriert werden, dass der BDC als Importserver fungiert. Dadurch werden sämtliche Systemrichtlinien und Logon Skripte auf den neuen BDC repliziert und können bei der Migration übernommen werden. Dabei ist zu beachten, dass die erste Replikation erst nach einiger Zeit erfolgt. Somit muss abgewartet werden bis das Verzeichnis repliziert wurde bevor mit dem Upgrade begonnen wird.

Abschließend sollte noch kontrolliert werden, ob mittels BDC auch auf alle Objekte wie Computer, User, Logon Skripte, Systemrichtlinien etc. zugegriffen werden kann.

7.3 Konfiguration des Systems, um es gegen eine Überlastung des PDC zu schützen

Da während und unmittelbar nach dem Upgrade lediglich ein Domänencontroller unter Windows Server 2003 existiert, kann es zu einer Überlastung dieses Domänencontrollers kommen. Dies geschieht dadurch, dass Windows 2000 und Windows XP Clients bei Erkennen eines Windows 2003 Domänencontrollers, ausschließlich diesen für die Authentifizierung benutzen. Dieses Verhalten wird von Microsoft als „Piling On" bezeichnet. Dabei ändert der Client ein Flag in seiner Sicherheitsdatenbank, wodurch die NTLM Authentifizierung deaktiviert und anstatt dieser nur noch die Kerberos Authentifizierung angewandt wird.

Aber nicht nur aus Gründen der Überlastung sollte die in diesem Punkt beschriebene Einstellung zur Anwendung kommen, sondern auch um einen

eventuellen Rückstieg auf das ursprüngliche System zu erleichtern. Da im Falle eines Rückstiegs kein Windows Server 2003 mehr zur Verfügung steht, kann sich ein Client nicht mehr an einem Windows NT 4.0 Domänencontroller anmelden.

Die Einstellung, dass sich ein Windows Server 2003 gegenüber Clients wie ein Windows NT 4.0 Server verhält, wird durch Erzeugen eines zusätzlichen Registrierungsschlüssels aktiviert. Dafür muss im Registrierungs-Editor im Ordner
HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
der Eintrag **NT4Emulator** als REG_DWORD mit dem Wert 1 erzeugt werden. Anschließend sollte der Server neu gestartet werden, damit die neuen Registrierungseinstellungen auch übernommen werden.

Weiters ist zu beachten, dass dieser Eintrag auf jedem zusätzlichen Domänencontroller, welcher der Domäne hinzugefügt wird erzeugt werden muss, um ein einheitliches Verhalten sämtlicher Domänencontroller zu bewirken. Für die Installation von Active Directory auf einem weiteren Server muss allerdings ein weiterer Eingriff in die Registrierung erfolgen. Da sich der Domänencontroller durch den gesetzten Schlüssel **NT4Emulator** wie ein Windows NT 4.0 Domänencontroller verhält, ist es für den neu zu installierenden Rechner nicht möglich sich an der Domäne zu authentifizieren, wodurch die Installation von Active Directory mit einem Fehler abgebrochen wird. Um den zusätzlichen Rechner die Möglichkeit der geforderten Authentifizierung zu geben, muss im Ordner
HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
der Eintrag **NeutralizeNT4Emulator** als REG_DWORD mit dem Wert 1 erstellt werden. Jetzt verläuft auch der Aufruf von DCPROMO auf dem neuen Domänencontroller problemlos und die Installation von Active Directory kann erfolgreich auf dem neuen Rechner durchgeführt werden. Dieser Registrierungseintrag kann nach erfolgter Installation wieder vom Domänencontroller entfernt werden, da sich Domänencontroller unter Windows Server 2003 untereinander ohnehin so verhalten als wäre dieser Registrierungseintrag gesetzt.

7.4 Hochstufung des BDC zum PDC

Vor der Hochstufung des BDC zum PDC muss eine vollständige Synchronisation aller Domänencontroller erfolgen, damit alle Domänencontroller über dieselben Informationen und Datenbanken verfügen. Weiters ist zu beachten, dass der BDC, der für die Hochstufung vorgesehenen ist, nicht als Exportserver für den LAN Manager Replikationsdienst konfiguriert ist. Sollte dies der Fall sein, muss dieser zuerst auf einen anderen Domänencontroller verlegt werden. Durch das Hochstufen eines BDC wird der PDC automatisch zu einem BDC heruntergestuft.

7.5 Kompatibilitätsprüfung

Bevor mit dem Update des Windows NT 4.0 Servers begonnen wird, sollte eine Überprüfung auf die Kompatibilität des Systems mit Windows Server 2003 erfolgen. Für diesen Zweck stellt Microsoft auf der Setup-CD des Windows Server 2003 ein Tool mit der Bezeichnung „Microsoft Windows Updateratgeber" zur Prüfung der Systemkompatibilität bereit. Dieses Werkzeug ermöglicht die Überprüfung des Systems auf eventuelle Inkompatibilitäten von Software- und Hardwarekomponenten mit der aktuellen Serverversion von Microsoft.

Abbildung 7.1: Startseite des Microsoft Windows-Updateratgeber

Zum Aufruf des Microsoft Windows Updateratgeber muss über die Kommandozeile in das Verzeichnis **I386** der Setup-CD gewechselt werden und anschließend der Befehl **winnt32 /checkupgradeonly** eingegeben werden.

Im Zuge der Kompatibilitätsüberprüfung können auch aktualisierte Setupdateien aus dem Internet geladen werden.

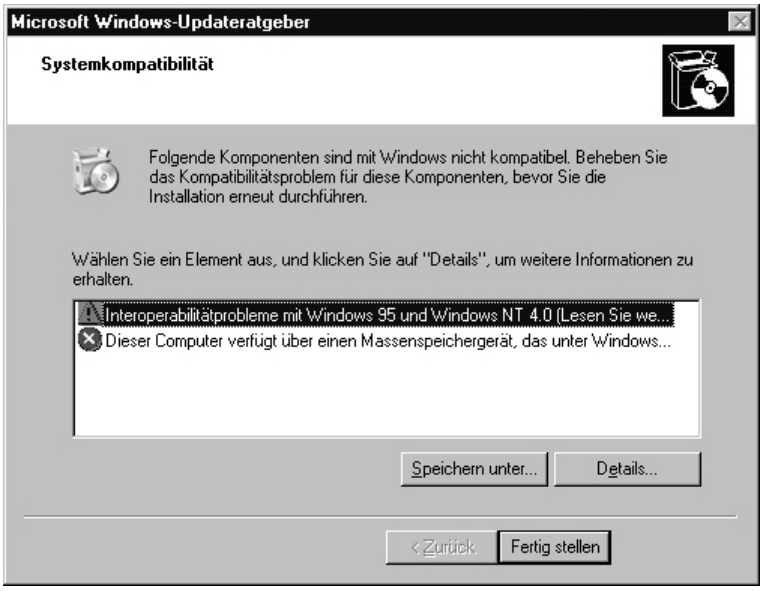

Abbildung 7.2: Mögliche Probleme (Microsoft Windows-Updateratgeber)

Nach der Überprüfung werden die möglichen Probleme aufgelistet. Mit der Schaltfläche *Details* können genaue Informationen zu den einzelnen Problemen abgerufen werden. Weiters besteht die Möglichkeit des Speicherns der dargestellten Probleme in einer .txt Datei.

Das in Abbildung 2.1 als erstes aufgelistete Problem stellt lediglich einen Warnhinweis auf mögliche Inkompatibilitätsprobleme mit älteren Betriebssystemen dar, da diese die neuen Sicherheitsmechanismen von Windows Server 2003 nicht unterstützen und somit unter Windows Server 2003 nicht korrekt funktionieren. Auf diese Inkompatibilität wird auch während der letztendlichen Installation von Microsoft Windows Server 2003 noch einmal hingewiesen.

Um einen erfolgreichen Abschluss der Installation von Windows Server 2003 zu ermöglichen, sollten die hier dargestellten Probleme vor Beginn eines Updates behoben werden und die Kompatibilitätsüberprüfung gegebenenfalls noch einmal ausgeführt werden.

7.6 Update des NT 4.0 Primary Domänencontrollers auf Windows 2003

Nachdem alle durch die Kompatibilitätsprüfung aufgelisteten Probleme behoben wurden, kann mit dem eigentlichen Update des Betriebssystems begonnen werden. Der Assistent zum Installieren von Windows Server 2003 kann über den Befehl **winnt32.exe** im Verzeichnis **I386** auf der Windows Server 2003 Setup-CD gestartet werden.

Abbildung 7.3: Startseite des Assistenten zum Installieren von Windows Server 2003

Auf der Startseite des Assistenten kann die gewünschte Installationsart ausgewählt werden. Hierbei wird automatisch die Installationsart Update vorgeschlagen. Es wird hier auch die Möglichkeit einer Neuinstallation geboten, welche aber für eine Migration nicht anwendbar ist, da dabei ansonsten sämtliche Domänendaten und Einstellungen verloren gehen würden.

Abbildung 7.4: Zustimmung zum Lizenzvertrag

Wie bei jeder Installation einer Software muss auch hier eine Zustimmung zum Lizenzvertrag erteilt werden und die Eingabe eines gültigen License-Keys erfolgen.

Abbildung 7.5: Eingabe des License-Keys

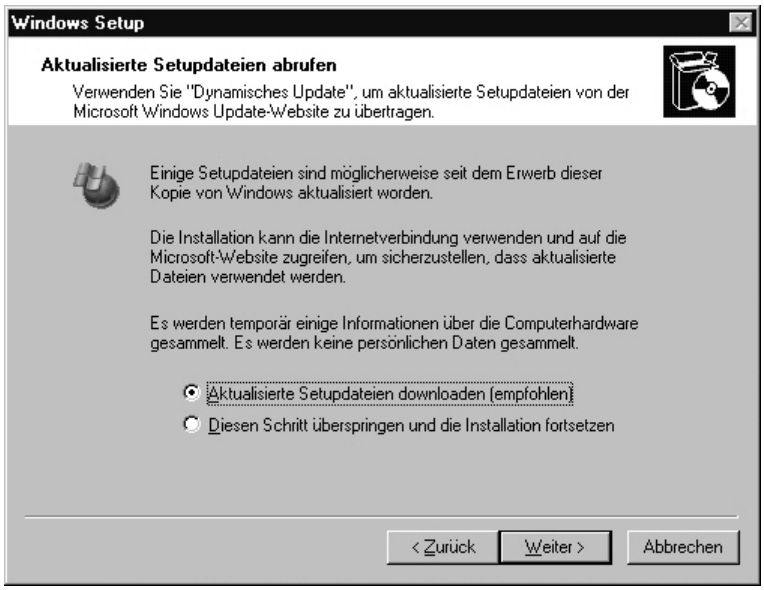

Abbildung 7.6: Abruf aktualisierter Setupdateien

Wie auch schon bei der vorangegangen Kompatibilitätsprüfung, besteht auch hier die Möglichkeit aktualisierte Setupdateien aus dem Internet herunterzuladen.

Im nachfolgenden Fenster wird nun noch einmal ein Hinweis auf eventuelle Kompatibilitätsprobleme angezeigt. Sind nach der Kompatibilitätsprüfung alle Probleme gelöst worden, sollte lediglich ein Hinweis auf die Inkompatibilität älterer Windows Versionen angezeigt werden.

Abbildung 7.7: Hinweis auf eventuelle Probleme während dem Update

7.7 Installation des Active Directory

Nach Abschließen des Updates auf Windows Server 2003 wird der Rechner neu gestartet und der Assistent zur Installation von Active Directory automatisch ausgeführt.

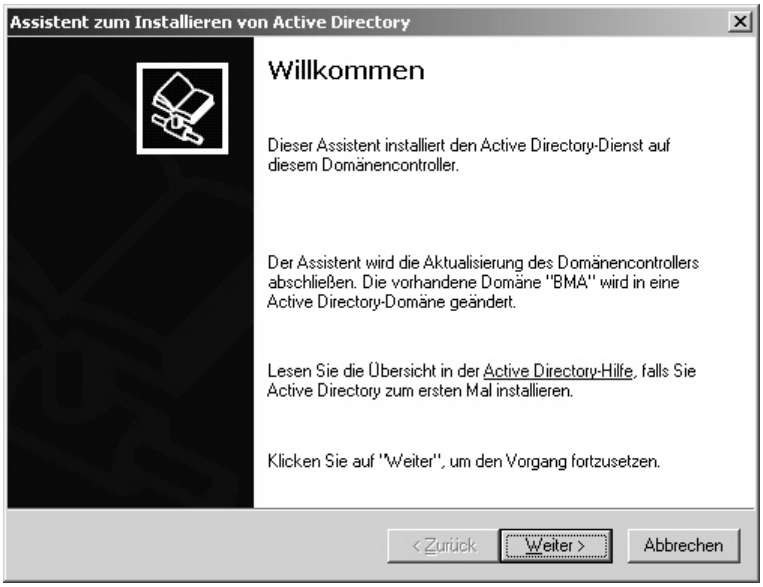

Abbildung 7.8: Startseite des Assistenten zum Installieren von Active Directory

Im nächsten Fenster weist der Assistent zum Installieren von Active Directory noch einmal auf eventuelle Inkompatibilitätsprobleme mit älteren Windows-Versionen hin.

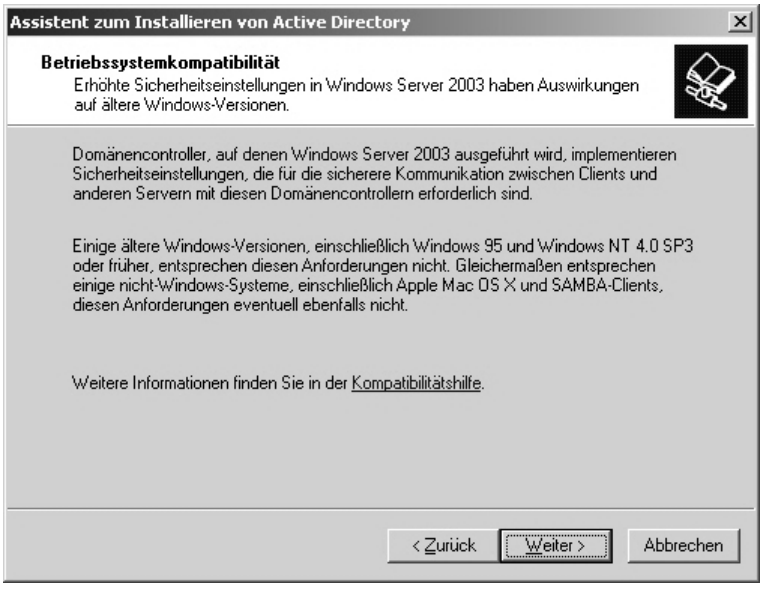

Abbildung 7.9: Betriebssystemkompatibilität mit älteren Windows Versionen

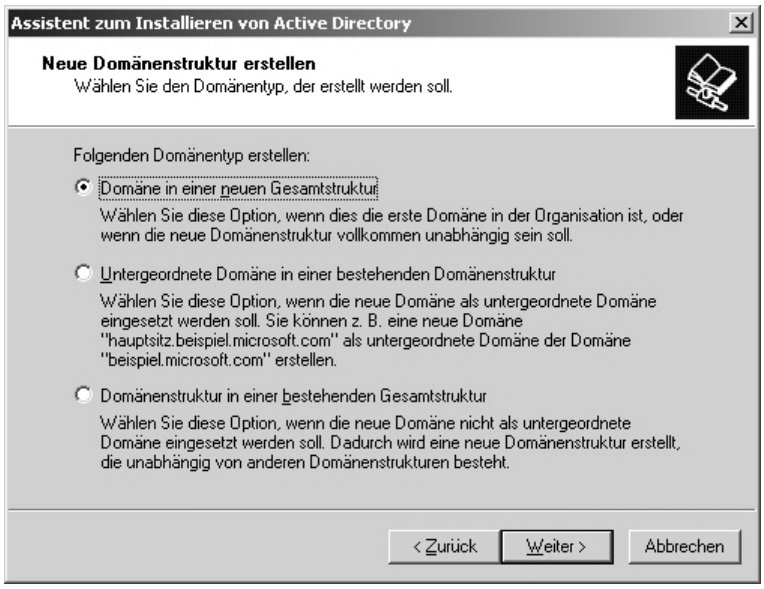

Abbildung 7.10: Auswahl der neuen Domänenstruktur

Hier kann nun entschieden werden, welche Domänenstruktur erstellt werden soll. Da es sich bei diesem Domänencontroller um den ersten in der neuen Domäne handelt und eine eigenständige Gesamtstruktur erzeugt werden soll, wird „Domäne in einer neuen Gesamtstruktur" ausgewählt.

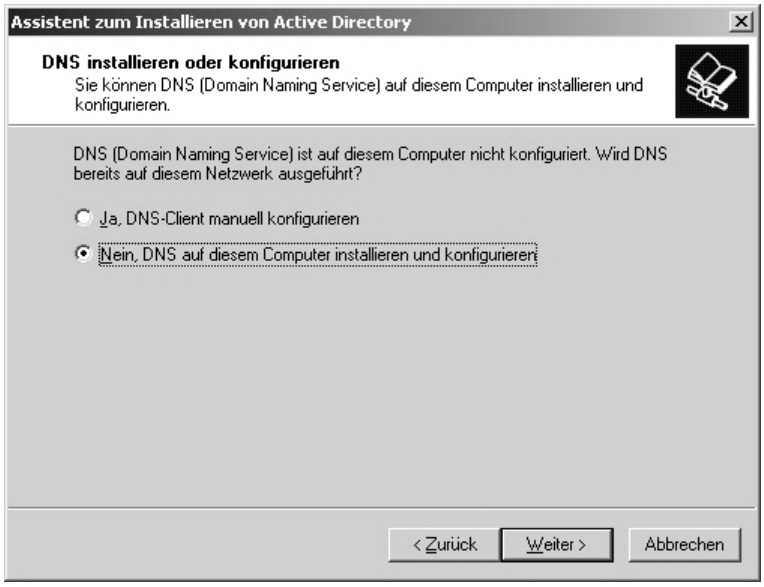

Abbildung 7.11: Auswahl zu Installation bzw. Konfiguration des DNS

Da die Implementierung des DNS Dienstes auch auf den neuen Domänencontroller erfolgen soll, wird in diesem Fenster die Option, dass DNS auf diesem Computer installiert und automatisch für die neue Domäne konfiguriert werden soll, ausgewählt.

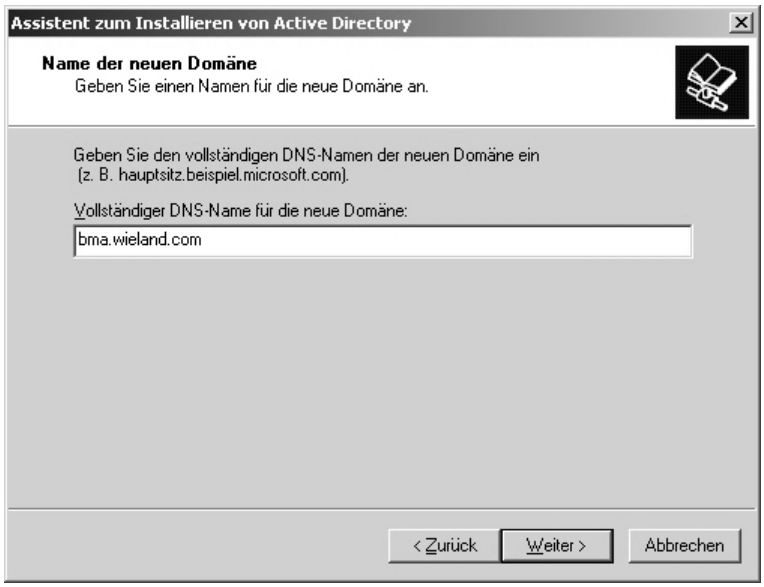

Abbildung 7.12: Auswahl des Namens für die neue Domäne

Um die bestehende Namenstruktur zu erhalten, wird bei der Auswahl des Namens der neuen Domäne der Name der bereits bestehenden Zone „bma.wieland.com" festgelegt.

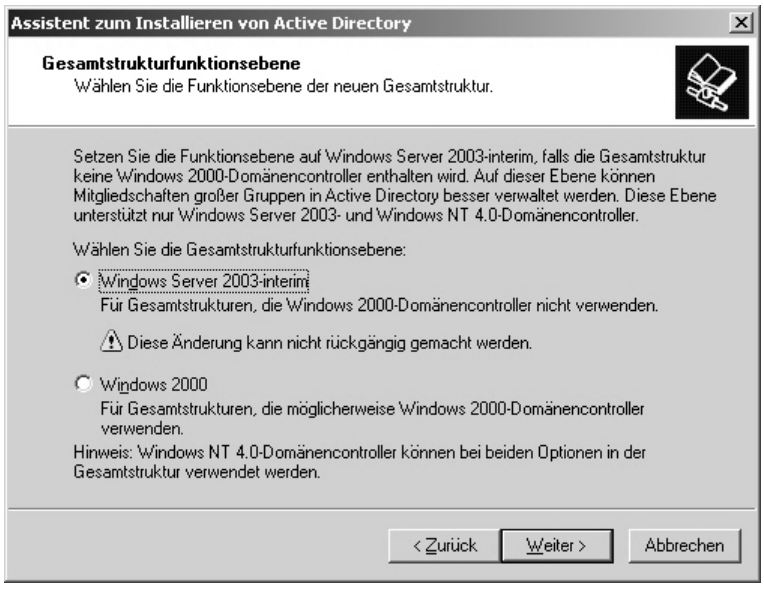

Abbildung 7.13: Auswahl der Gesamtstrukturfunktionsebene

Nachdem in Zukunft kein Einsatz von Domänencontrollern unter Windows 2000 geplant ist, wird der Modus der Gesamtstrukturfunktionsebene auf Windows Server 2003-interim ausgewählt. Wie in Abbildung 7.13 dargestellt, können Windows NT 4.0 Domänencontroller bei beiden Optionen verwendet werden.

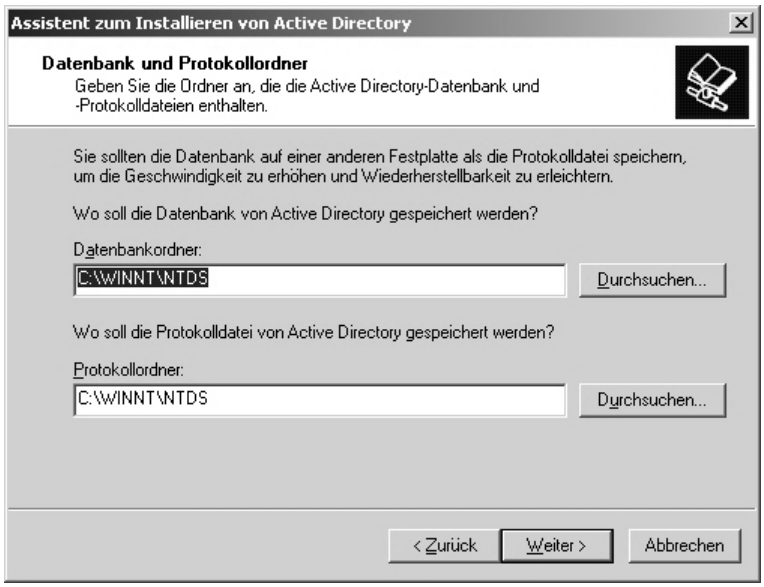

Abbildung 7.14: Festlegen der Speicherorte für die Datenbank und Protokolle

Für die Festlegung des Speicherortes von Datenbank- und Protokollordner werden die vom Assistenten vorgeschlagenen Standardorte beibehalten. Diese können bei Notwendigkeit auch nachträglich noch verändert werden.

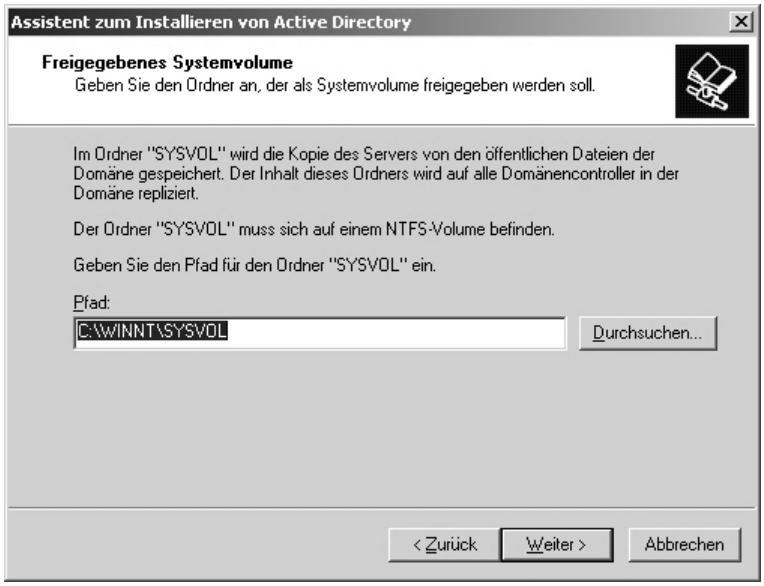

Abbildung 7.15: Festlegen der Freigabe des Systemvolume

Auch bei der Festlegung des Ordners für das freigegebene Systemvolume wird die Standardeinstellung beibehalten.

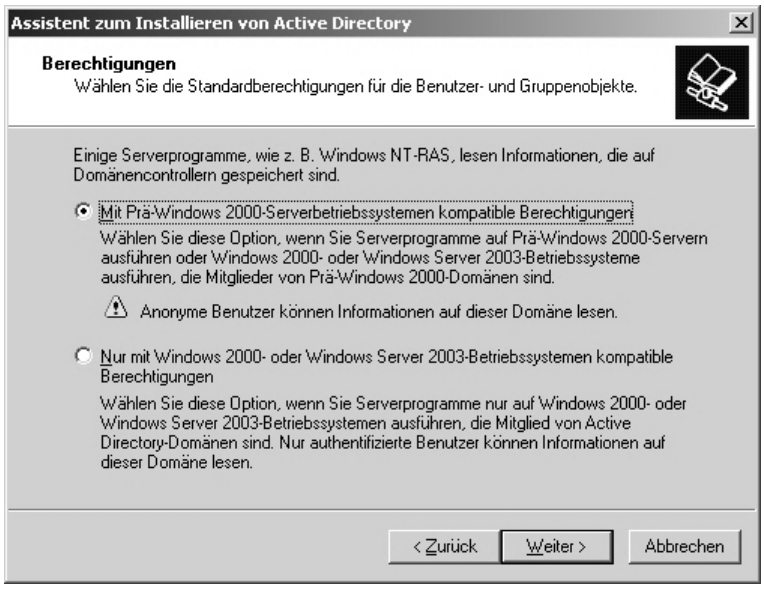

Abbildung 7.16: Festlegen der Freigabe des Systemvolume

Da die Auswirkungen auf Dienste und Anwendungen bei Wahl der zweiten Option nicht exakt abgeschätzt werden können, wird sicherheitshalber die Option „Mit Prä-Windows 2000-Serverbetriebssystem kompatible Berechtigungen" ausgewählt. Dies wird nach Abschluss der Migration weiter überprüft und wenn möglich korrigiert werden, da diese Option ein gewisses Sicherheitsrisiko birgt.

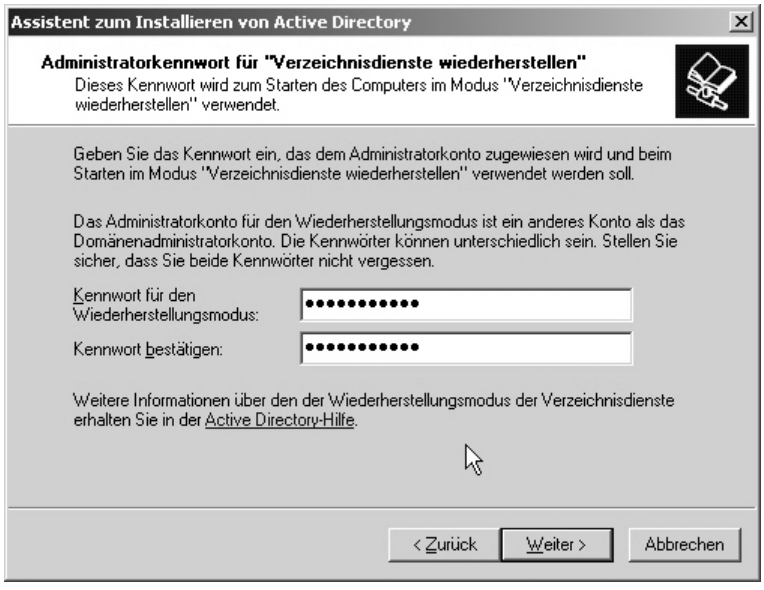

Abbildung 7.17: Festlegen des Kennworts für den Wiederherstellungsmodus

Um den Domänencontroller im Modus „Verzeichnisdienste wiederherstellen" starten zu können, muss ein Kennwort für diesen Modus definiert werden.

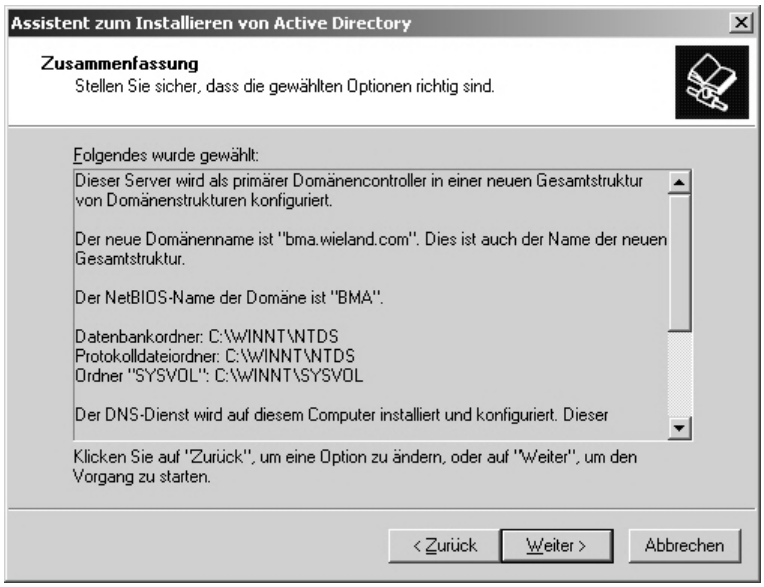

Abbildung 7.18: Zusammenfassung des Assistenten

Bevor die getroffenen Einstellungen zur Anwendungen kommen, können diese auf der Seite *Zusammenfassung* des Assistenten zum Installieren von Active Directory noch einmal überprüft werden. Mit einem Klick auf die Schaltfläche „Weiter" wird die Installation der diversen Dienste und des Active Directory gestartet. Dieser Vorgang kann einige Zeit in Anspruch nehmen.

Abbildung 7.19: Fertigstellen des Assistenten

Nach Abschluss der Installation von Active Directory wird noch ein abschließender Hinweis bezüglich der korrekten Installation von Active Directory auf diesem Computer ausgegeben.

7.8 Anpassung des DHCP Dienstes

Da im Moment keine Änderung des DHCP Dienstes durchgeführt werden soll und auch auf die Einführung einer Redundanz vorläufig verzichtet wird, sind kaum Änderungen des DHCP Dienstes auf dem Server r13s02.bma.wieland.com notwendig.

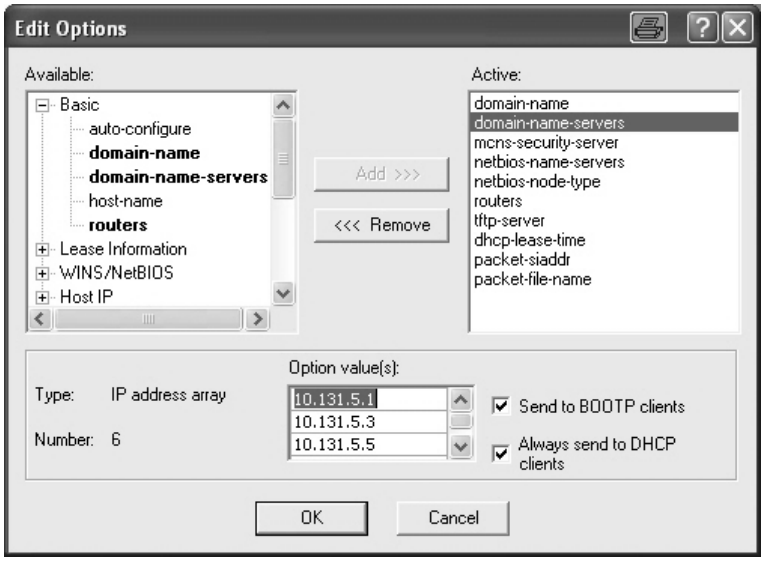

Abbildung 7.20: Anpassung der DHCP Optionen

Somit muss lediglich eine Anpassung der DHCP Optionen durchgeführt werden (s. Abbildung 7.20). Diese ist notwendig, da sämtliche Clients die Konfiguration der DNS Server per DHCP beziehen und der DNS Dienst, wie im folgenden Punkt beschrieben, an die neuen Verhältnisse angepasst werden muss.

7.9 Anpassung des bestehenden DNS Dienstes

Da im ursprünglichen System bereits ein DNS Server implementiert war und dieser als strategisches Produkt der Konzernleitung gilt und somit auch weiterhin seinen Dienst verrichten soll, muss dieser für die Zusammenarbeit mit dem neuen auf dem Domänencontroller integrierten DNS Server, angepasst werden. Die DNS Server auf den neuen Domänencontroller sollen dabei lediglich der notwendigen Fehlertoleranz dienen, damit bei Ausfall des primären DNS Servers r13s02.bma.wieland.com DNS Abfragen weiterhin bearbeitet werden können und nicht für jede Abfrage auf sekundäre DNS Server in der Konzernleitung zugegriffen werden muss.

Dabei muss nun auf den neuen Domänencontroller die Zone bma.wieland.com als sekundäre Zone eingerichtet werden. An der Konfiguration aller anderen Zonen wird vorläufig keine Änderung durchgeführt.

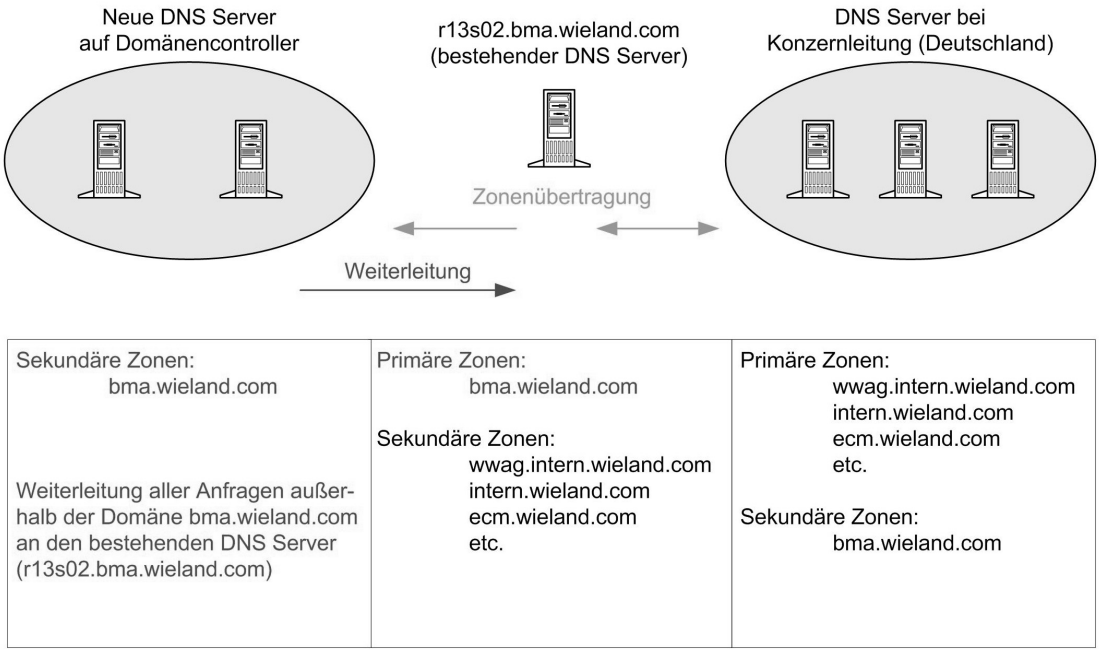

Abbildung 7.21: Änderung der DNS Infrastruktur

Wie in vorangegangener Abbildung dargestellt, sind auf dem Server r13s02.bma.wieland.com keine wesentlichen Änderungen notwendig. Auf den neuen DNS Servern muss hingegen die Zone bma.wieland.com als sekundäre Zone eingerichtet werden.

Für Anfragen, welche die neuen DNS Server der Domäne bma.wieland.com nicht beantworten können, muss eine Weiterleitung dieser Anfragen an den bestehenden DNS Server r13s02.bma.wieland.com konfiguriert werden, da dieser nach wie vor durch regelmäßige Zonenübertragungen sämtliche von der Konzernleitung verwalteten Zonen auflösen kann.

Um den Domänencontrollern die einwandfreie Registrierung ihrer Dienste auf dem DNS Server Cisco Network Registrar zu ermöglichen, muss auf diesem noch eine kleine Änderung erfolgen. Dabei müssen für die Zone bma.wieland.com dynamische Updates von den Domänencontrollern akzeptiert werden. Dies wird durch einfache Angabe der beiden IP-Adressen der neuen Server erreicht.

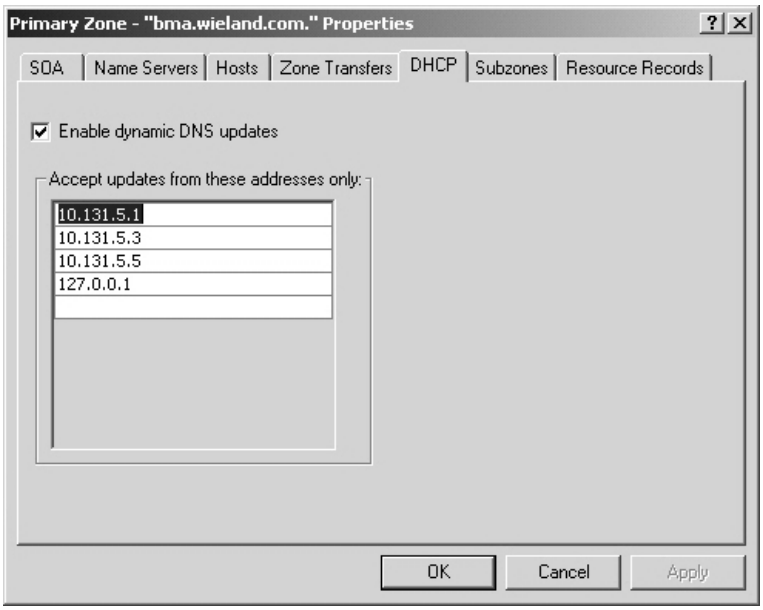

Abbildung 7.22: Konfiguration dynamischer DNS Updates

7.9.1 Installation des DNS Dienstes

Die Funktion eines DNS Servers auf den neuen Domänencontrollern kann unter **Start → Serververwaltung → Funktion hinzufügen oder entfernen** einem Domänencontroller hinzugefügt werden.

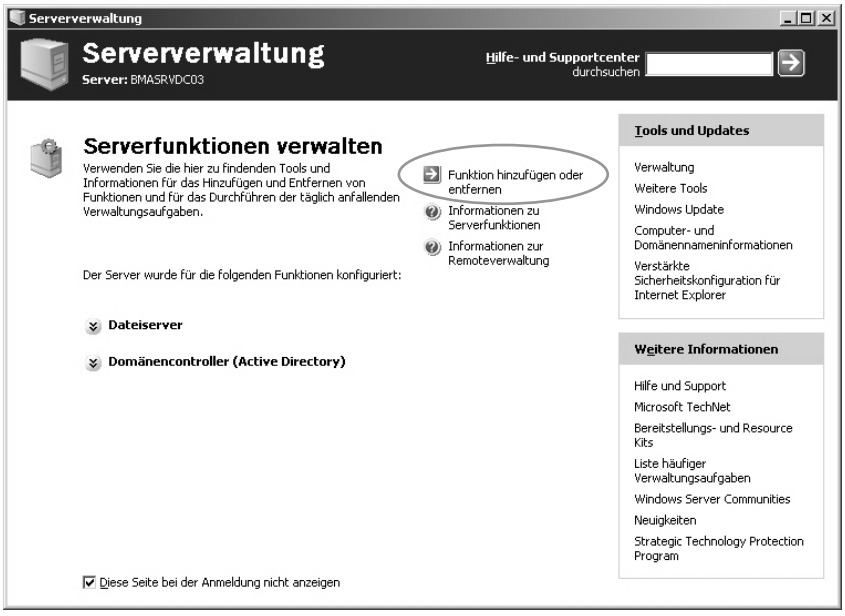

Abbildung 7.23: Serverfunktionen verwalten (Servermanager)

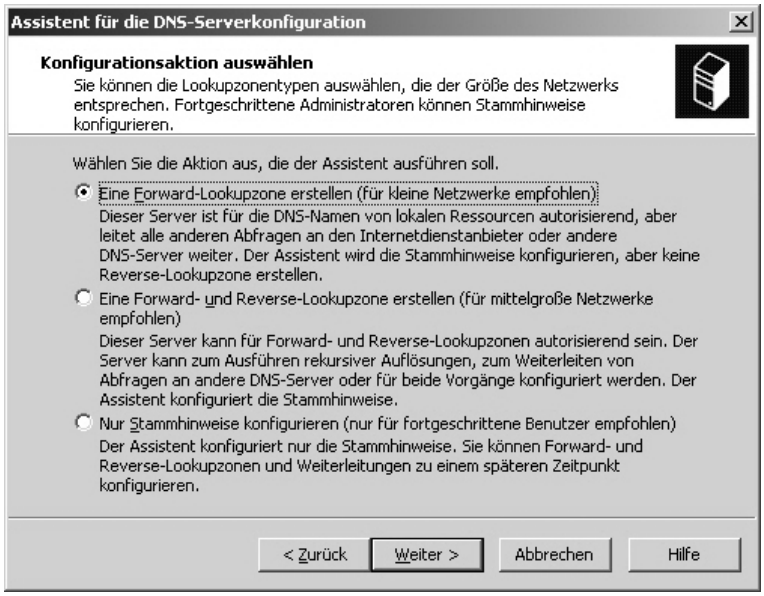

Abbildung 7.24: Auswahl der Zonen-Art

Gleich anschließend nach der Installation des DNS Dienstes kann eine Konfiguration einer neuen DNS Zone vorgenommen werden, wobei zuerst festgelegt wird, welche Zone erstellt werden soll.

Im nächsten Schritt wird definiert, ob dieser Server die Zone verwaltet oder ob er diese von einem anderen Server importiert. In Fall der Buntmetall Amstetten GmbH wird diese vom bestehen Server r13s02.bma.wieland.com importiert.

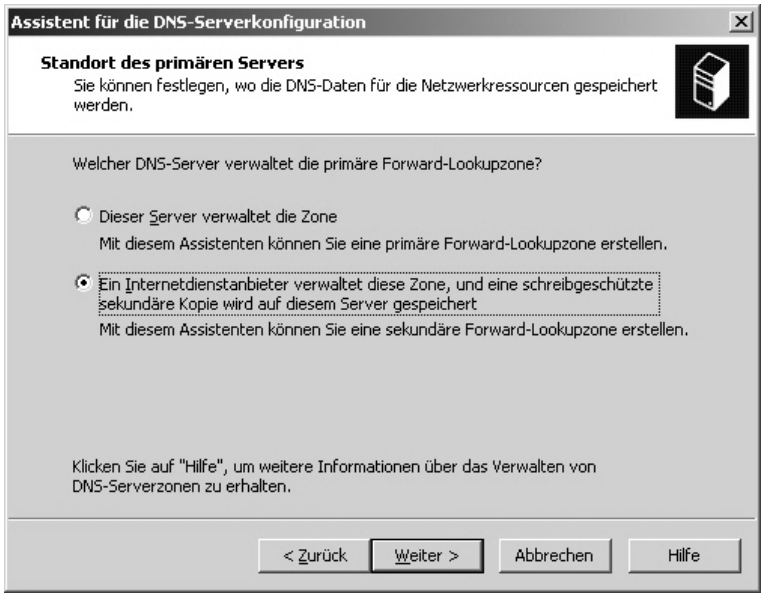

Abbildung 7.25: Festlegung von primär bzw. sekundär

Abbildung 7.26: Definition des Zonen Namens

Anschließend muss der Name der zu importierenden Zone definiert werden.

Nun muss die IP-Adresse des Server eingegeben werden, von welchem die Zone importiert werden soll, in diesem Fall jene des Server r13s02.bma.wieland.com mit der Adresse 10.131.5.1.

Abbildung 7.27: Definition des primären Server für die Zone

Abschließend kann noch definiert werden, ob dieser Server Anfragen welcher er nicht beantworten kann weiterleiten soll und wohin diese weitergeleitet werden sollen. Auch hier wird in diesem Fall die IP-Adresse des Servers r13s02.bma.wieland.com angegeben.

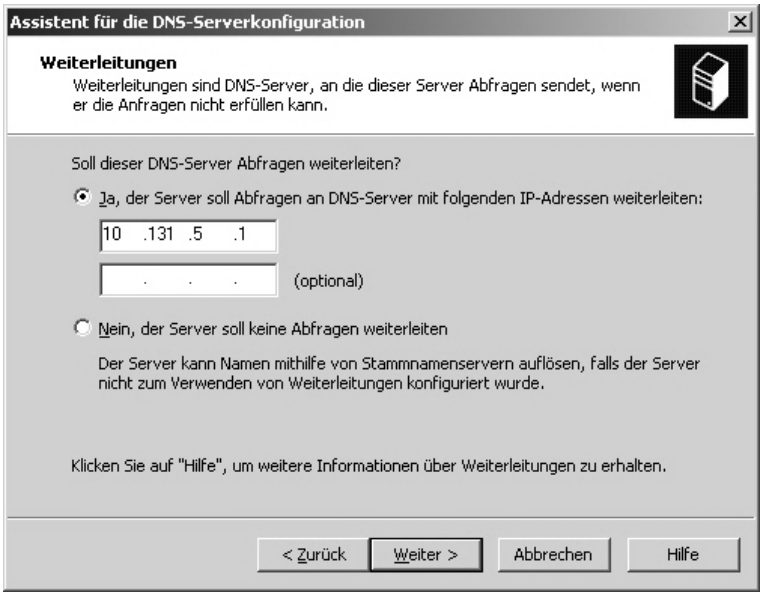

Abbildung 7.28: Konfiguration einer Weiterleitung

Eine abschließende Zusammenfassung und Bestätigung der getätigten Konfiguration richtet die Zone bma.wieland.com auf dem neuen Server ein.

Analog zu dieser Konfiguration kann nun auch die Reverse-Lookupzone, welche ebenfalls auf dem bestehenden DNS Server r13s02.bma.wieland.com auf den neuen DNS Servern eingerichtet werden.

7.10 Konfiguration des Windows-Zeitdienstes

„Für eine ordnungsgemäße Funktionsfähigkeit sind eine Reihe von Komponenten der Windows Server 2003-Produktfamilie auf eine genaue und synchronisierte Zeit angewiesen. Wenn beispielsweise die Systemuhren nicht auf allen Computern auf die richtige Uhrzeit synchronisiert sind, kann das Kerberos V5-Authentifizierungprotokoll Anmeldeanforderungen fälschlich als Eindringversuche interpretieren und Benutzern den Zugang verweigern.“ (Microsoft, 2006 d).

Solange die Konfiguration des Windows Zeitdienstes nicht durchgeführt wurde, wird ein Warnhinweis in das Ereignisprotokolls des Domänencontrollers ge-

schrieben. Um eine konsistente Zeit im Netzwerk zu garantieren, muss der Domänencontroller für die Synchronisation mit einer zuverlässigen NTP Quelle (Network Time Protocol) konfiguriert werden.

Da dieser Dienst auch im ursprünglichen System bereits konfiguriert war, wird die bestehende Konfiguration auch weiterhin verwendet werden. Dabei ist eine Synchronisation mit dem Server 10.34.5.177 zu definieren.

Nachfolgende Schritte sind zur Konfiguration des Windows Zeitdienstes notwendig:

- Anmeldung auf dem Domänencontroller
- Über die Befehlszeile muss folgender Befehl eingegeben werden:
    - w32tm /config /manualpeerlist:10.34.5.177 /syncfromflags:manual /reliable:yes
- Abschließend muss der Zeitdienst noch neu gestartet werden:
    - net stop w32time
    - net start w32time

Dieser Schritt ist nur auf jenem Domänencontroller mit der Rolle des PDC-Emulators durchzuführen, da alle anderen Domänencontroller automatisch aufgrund der Domänenhierarchie den PDC-Betriebsmaster des Gesamstrukturstammes als autorisierende Zeitquelle verwenden.

7.11 Aktualisierung zusätzlicher Domänencontroller

Um die notwendige Redundanz bzw. Fehlertoleranz für Clients zu schaffen, sollten zusätzliche Domänencontroller unter Microsoft Windows Server 2003 installiert werden. Dies kann dabei durch Aktualisierung der restlichen BDCs oder durch Hinzufügen von Mitgliedsservern und Installation von Active Directory auf diesen erfolgen.

Aufgrund der unzureichenden Hardwarekonfiguration der verbleibenden BDCs (s. Punkt 2.4) kann lediglich der Server srv_bma_00 für die Installation als Domänencontroller herangezogen werden. Dieser wird aber nicht durch ein Upgrade des Betriebssystems, sondern durch eine Neuinstallation von Win-

dows Server 2003 in die neue Umgebung übernommen. Dies wird allerdings erst einige Tage nach Beginn der Migration erfolgen, da dieser die Funktion eines BDCs, um gegen eventuell auftretende Probleme gerüstet zu sein, behält.

Aus diesem Grund wird unmittelbar nach der Migration des PDCs ein zusätzlicher Domänencontroller auf einem neu installierten Mitgliedsserver aufgesetzt (srvbmadc02.bma.wieland.com). Dieser wird auch nach der Neuinstallation des Servers srv_bma_00 seine Funktion als zusätzlicher Domänencontroller behalten und somit die notwendige Fehlertoleranz bzw. Ausfallsicherheit für den letztendlichen Betrieb der neuen Domäne bereitstellen.

8 Sicherstellung der Netzwerkdienste während dem Update

Da das Ziel jeder Umstellung bzw. Einführung eines neuen Systems, die bestmögliche Aufrechterhaltung sämtlicher Dienste und Funktionen einer Umgebung darstellt, sollen in diesem Abschnitt die einzelnen Dienste und die zur Sicherstellung erforderlichen Maßnahmen näher untersucht werden. Die nachfolgend aufgelisteten Punkte sollen dazu dienen, den Anwendern den unterbrechungsfreien Zugriff auf sämtliche Ressourcen zu ermöglichen.

8.1 Sicherstellung des DNS Dienstes

Wie schon in einigen Punkten erwähnt, ist der DNS Dienst auf einem eigenständigen Server r13s02.bma.wieland.com mittels der Software Cisco Network

Registrar 5.5.9 implementiert. Weiters unterstützt dieser auch sämtliche Anforderungen zur Integration in eine Active Directory Struktur (s. Punkt 4.3). Da dieser somit von der Umstellung nicht betroffen ist und zudem nur geringfügige Anpassungen zur Unterstützung des neuen Systems durchgeführt werden müssen, sind keine besonderen Maßnahmen zur Sicherstellung des DNS Dienstes während dem Update vorzusehen.

8.2 Sicherstellung des NetBIOS Dienstes

Grundsätzlich sind bei einem Upgrade der Domäne von Windows NT 4.0 auf Windows Server 2003 keine Auswirkungen auf den bestehenden WINS Dienst zu erwarten. Da sich dieser Dienst im Fall der Firma Buntmetall Amstetten GmbH auf dem Server srv_bma_00 befindet, welcher im Zuge der Migration mittels Neuinstallation zu einem zusätzlichen Domänencontroller der Domäne hinzugefügt werden soll, müssen gewisse Maßnahmen getroffen werden um die Sicherstellung dieses Dienstes zu gewährleisten. Grundsätzlich ist in einer auf Windows Server 2003 umgestellten Umgebung die Aufrechterhaltung des WINS Dienstes nicht notwendig, da diese ausschließlich auf DNS basiert. Da jedoch im alten System die Wartung dieses Dienstes durch die Konzernzentrale in Deutschland erfolgte, muss die Stilllegung des Dienstes in Abstimmung mit der Konzernzentrale erfolgen.

Deshalb wird im Zuge der Umstellung der Domäne eine Verlegung des WINS-Dienstes vom Server srv_bma_00 auf den neuen Domänencontroller srvbmadc02.bma.wieland.com erfolgen. Für die Clients ergibt sich dadurch keine wesentliche Problematik, da diese die Adresse des primären WINS-Servers per DHCP zugewiesen bekommen. Daraus resultiert, dass auf dem DHCP Server Cisco Network Registrar die DHCP Option für den NetBIOS-Name-Server von der Adresse 10.131.5.5 auf 10.131.5.3 geändert werden muss. Somit wird sämtlichen Clients bei einem Neustart bzw. nach Ablauf der Lease automatisch die neue Adresse zugewiesen. Mit der Konzernleitung muss nun noch die Replikation der WINS-Server aktualisiert werden, damit dieser WINS-Server als neuer Replikationspartner eingetragen und auch nach wie vor zur Replikation mit dem WINS-Server seitens der Konzernleitung im Stande ist.

8.3 Sicherstellung des DHCP Dienstes

Auch hier gilt selbiges wie im Punkt 8.1 beschrieben. Da auch der DHCP Dienst auf dem Server r13s02.bma.wieland.com ausgeführt wird, sind keine Maßnahmen zur Aufrechterhaltung des DHCP Dienstes während dem Update erforderlich.

8.4 Unterstützung der LAN Manager Replikation

Unter Windows NT 4.0 wird das LAN Manager Replication Service für die Synchronisation der Systemrichtlinien und Logon-Scripts zwischen den Domänencontrollern verwendet. Da dieser Dienst in einer Windows Server 2003 Umgebung nicht mehr existiert, müsste für den Betrieb im gemischten Modus (paralleler Betrieb von Windows NT 4.0 und Windows Server 2003 Domänencontroller) eine Lösung bereitgestellt werden, welche die Synchronisation zwischen einem Windows Server 2003 Domänencontroller und einem noch vorhandenen Windows NT 4.0 BDC ermöglicht. Da im Fall der Firma Buntmetall Amstetten GmbH die Migration so rasch wie möglich erfolgen soll und eine einheitliche Umgebung (ausschließlicher Betrieb von Windows Server 2003 Domänencontrollern) angestrebt wird, muss dieser Punkt nicht näher berücksichtigt werden. Es muss allerdings darauf geachtet werden, dass solange ein Windows NT 4.0 BDC existiert, auf diesen keine Änderungen an Systemrichtlinien bzw. Logon-Skripten durchgeführt wird. Diese Änderungen würden aufgrund der fehlenden Synchronisation nicht auf die neuen Windows Server 2003 Domänencontroller repliziert werden.

8.5 Unterstützung von RAS Diensten

Wie aus dem Punkt 2.6 hervorgeht, ist der RAS Dienst der aktuellen Umgebung auf dem Server srv_bma_05.bma.wieland.com implementiert. Weiters ist aus der vorangegangenen Analyse der bestehenden Infrastruktur ersichtlich, dass dieser bereits auf einem Windows Server 2003 installiert ist und somit keine Beeinträchtigungen bei der Migration zu erwarten sind. Da aber zum gegenwärtigen Zeitpunkt noch keine Entscheidung existiert, ob der RAS Dienst überhaupt noch verwendet wird, kann von der genaueren Untersuchung dieses Punktes Abstand genommen werden.

8.6 Planung der Unterstützung von Gruppen- bzw. Systemrichtlinien

Eine der wesentlichsten Erneuerungen von Microsoft Windows Server 2003 und der Einführung von Active Directory ist die Möglichkeit der Gruppenrichtlinien. Da in einer Umgebung von Windows NT 4.0 lediglich Systemrichtlinien zum Einsatz kommen, müssen Überlegungen stattfinden, die einen Übergang von Systemrichtlinien auf Gruppenrichtlinien regeln.

Im Fall der Firma Buntmetall Amstetten GmbH muss eine Lösung implementiert werden, welche sowohl Systemrichtlinien als auch Gruppenrichtlinien zur Verfügung stellt. Dies ist notwendig, da in der aktuellen Netzwerkumgebung Clients unter Windows NT 4.0 und unter Windows XP im Einsatz sind. Dabei erhalten die Windows NT4.0 Clients Systemrichtlinien zugewiesen und Windows XP Clients Gruppenrichtlinien.

8.6.1 Systemrichtlinien

Während einer Migration werden die auf den bestehenden Windows NT 4.0 Domänencontrollern vorhandenen Systemrichtlinien automatisch in die NETLOGON Freigabe des neuen Systems übernommen. D.h., dass Clients mit Betriebssystemen vor Windows 2000 nach wie vor ihre Systemrichtlinien von dem jeweils verfügbaren Anmeldeserver beziehen können. Auch hier kommt wieder der Aspekt der fehlenden Synchronisation zwischen neuen Active Directory Domänencontroller und BDC, welcher schon im Punkt 8.4 beschrieben wurde, zu tragen. Da bei der Firma Buntmetall Amstetten GmbH ohnehin keine Änderungen an Systemrichtlinien geplant sind, muss darauf aber nicht weiter Rücksicht genommen werden.

Weiters wurde bereits mit dem Austausch der noch bestehenden Windows NT 4.0 Clients begonnen. Somit ist in naher Zukunft damit zu rechnen, dass sämtliche Windows NT 4.0 Clients durch neue Windows XP Clients abgelöst werden. Einstellungen welche mittels Systemrichtlinien getätigt wurden, haben permanenten Charakter, d.h., dass diese auf dem jeweiligen Rechner verbleiben und auch bei Ausloggen des Users nicht verworfen werden. Aus diesem Grund kann auch von einer zukünftigen Implementierung von Systemrichtlinien abgesehen werden, da die bestehenden Windows NT 4.0 Clients die relevanten Einstellungen bereits erhalten haben und die Installation von neuen Windows NT 4.0 Clients ausgeschlossen werden kann.

8.6.2 Gruppenrichtlinien

Wie schon oben erwähnt wurde, stellen Gruppenrichtlinien eine der wesentlichsten Erneuerungen im neuen System dar und schaffen eine Menge von Möglichkeiten bzw. Vorteilen. Da Clients ab dem Betriebssystem Windows 2000 in einer Active Directory Umgebung keine Systemrichtlinien mehr interpretieren, muss eine Implementierung von Gruppenrichtlinien angestrebt werden. Auch hier gilt das permanente Verhalten von bereits angewandten Systemrichtlinien. Dies hat zur Folge, dass sämtliche Clients mit Betriebssystemen ab Windows 2000, welche in der ursprünglichen Domäne bereits Systemrichtlinien verarbeitet haben, diese Einstellungen dauerhaft in der Registrierung eingetragen haben. Somit müssen speziell für neu installierte Clients die notwendigen Konfigurationen durch Einrichtung von Gruppenrichtlinien zur Verfügung gestellt werden.

Für die Erstellung von Gruppenrichtlinien bieten sich grundsätzlich zwei Möglichkeiten. Einerseits ist es möglich, die bestehenden Systemrichtlinien mit dem Tool gpolmig.exe aus dem Windows 2000 Resource Kit in Gruppenrichtlinien umzuwandeln. Andererseits kann eine manuelle Erstellung und somit gleichzeitige Überarbeitung der gewünschten Gruppenrichtlinien erfolgen.

8.7 Migration der Logon-Skripte

Während des Upgrades des primären Domänencontrollers von Windows NT 4.0 auf Windows Server 2003 werden sämtliche Logon-Skripte automatisch in die NETLOGON Freigabe des neuen Domänencontrollers übernommen. Somit sind keine Auswirkungen auf die bestehenden Logon-Skripte zu erwarten und die Clients werden diese nach wie vor verarbeiten.

8.8 Auswirkungen auf Ressourcen Zugriff

Auch dieser Punkt ist ähnlich dem vorangegangen Punkt zu betrachten, da während der Migration sämtliche für den Ressourcen Zugriff relevanten Komponenten aufrechterhalten bleiben. Diese Komponenten umfassen:

- Security Identifieres (SIDs): Sämtliche in Active Directory enthaltenen Objekte behalten ihre SID

- Gruppenmitgliedschaft: Benutzerkonten welche Mitglieder einer Gruppe sind, sind auch nach Migration Mitglied dieser Gruppe
- Berechtigungen auf Freigaben und das Dateisystem: Sämtliche Zugriffsberechtigungen auf Freigaben und Ordner bleiben bei der Migration erhalten
- Registrierungsberechtigungen: Zugriffsberechtigungen auf die Registrierung bleiben erhalten
- Vertrauensstellungen: Vertrauensstellungen mit anderen Domänen bleiben erhalten

8.9 Migration von Vertrauensstellungen

Die Migration der Domäne von einer Windows NT 4.0 Umgebung in eine Windows Server 2003 Umgebung hat keine wesentlichen Auswirkungen auf eine bestehende Vertrauensstellung. Diese werden automatisch in das neue System übernommen. Aus diversen Literaturen geht aber hervor, dass diese nach Abschluss einer Migration neu erstellt werden sollen.

8.10 Migration der User Profile

Wie auch schon bei den Logon-Skripten sind auch hier keine Auswirkungen auf die bestehenden User Profile zu erwarten. Auf diese kann auch nach Migration problemlos über den Pfad, welcher jedem Benutzerkonto in Active Directory zugewiesen wurde und welcher während einer Migration erhalten bleibt, zugegriffen werden.

8.11 Auswirkungen auf firmenspezifische Anwendungen

Da es bei der Firma Buntmetall Amstetten GmbH einige betriebsnotwendige Dienste und Anwendungen gibt, welche den Usern verschiedenste Funktionen zur Verfügung stellen, müssen auch für diese, soweit dies möglich ist, die Auswirkungen und die zu erwartenden Probleme ausgewertet werden. Dies ist

zum Teil in der praktischen Testumgebung erprobt worden. Da für diese Testumgebung aber nur begrenzte Ressourcen zu Verfügung standen, wurde die Untersuchung der Auswirkungen auf die für den Betrieb wesentlichsten Anwendungen und Dienste beschränkt.

8.11.1 Lotus Notes

Bei der Firma Buntmetall Amstetten GmbH kommt für die Kommunikation per Mail Lotus Notes zum Einsatz. Da diese Anwendung für den ordnungsgemäßen Betrieb unabdingbar ist, muss die Sicherstellung dieser Anwendung gewährleistet werden.

Bei einer Analyse der Software konnte festgehalten werden, dass die Funktion von Lotus Notes in keinem unmittelbaren Zusammenhang mit den Funktionen einer Microsoft Umgebung steht. Für die Authentifizierung werden dabei eigene Benutzerkonten auf dem Server für Lotus Notes erzeugt, welche in keiner Verbindung mit den Benutzern des zukünftigen Active Directory stehen. Die Kommunikation zwischen Server und Client erfolgt dabei über TCP/IP. Aufgrund dieser Erkenntnisse kann vorausgesetzt werden, dass für den Betrieb von Lotus Notes in der neuen Umgebung keine Auswirkungen zu erwarten sind. Dies konnte auch durch einen Test in der implementierten Testumgebung bestätigt werden.

8.11.2 SAP

Als weitere sehr wesentliche Anwendung für Geschäftsprozesse kommt bei der Firma Buntmetall Amstetten GmbH die Unternehmens-Lösung SAP zum Einsatz. Diese wird allerdings nicht lokal bereitgestellt, sondern wird seitens der Konzernleitung in Deutschland angeboten und auch administriert.

Da auch hier die gesamte Kommunikation per TCP/IP abgewickelt wird, kann davon ausgegangen werden, dass eine Migration ebenfalls keine Auswirkungen auf den ordnungsgemäßen Betrieb mit sich bringt. Aufgrund eines kurzen Probetriebs in der aufgebauten Testumgebung, konnte auch diese Behauptung verifiziert werden.

8.11.3 Oracle Datenbanken

Für die Speicherung diverser Produktionsdaten ist in der Infrastruktur der Firma Buntmetall Amstetten GmbH ein Oracle Datenbank Cluster implementiert.

Wie auch schon in den beiden vorangegangenen Punkten, kann auch hier davon ausgegangen werden, dass keine Auswirkungen auf das bestehende System zu erwarten sind. Zumal die Datenbankinstallation von Oracle ebenfalls in keinem Zusammenhang mit den von Microsoft implementierten Funktionen steht.

8.11.4 Produktionsspezifische Anwendungen

Für die Produktionsumgebung der Firma Buntmetall Amstetten sind einige eigenständig entwickelte Software-Lösungen im Einsatz. Da diese ebenfalls lediglich über TCP/IP kommunizieren, wird davon ausgegangen, dass keine Beeinträchtigungen durch eine Migration zu erwarten sind.

Für alle weiteren Anwendungen und Dienste wurde von einer genaueren Betrachtung abgesehen. Der Grund dafür ist, dass diese als eher unkritisch für den laufenden Betrieb angesehen werden bzw. ein Test in der Produktionsumgebung mit den vorhandenen Mitteln nicht ohne zu großem Aufwand durchgeführt werden konnte.

9 Gewinnbringende Aspekte und Ausblick

Abschließend sollen in diesem Kapitel die aufgrund der Durchführung einer Migration entstandenen Vorteile und gewonnenen Möglichkeiten betrachtet werden. Hierbei sollen die neuen und verbesserten Technologien, welche durch die Umstellung auf das neue System zur Verfügung stehen, erfasst werden.

9.1 OU–Struktur (Organizational Unit)

Ein wesentliches Kriterium für eine angemessene Verwaltung der Domäne stellt eine an die Organisation des Unternehmens angepasste OU-Struktur dar. Anhand einer gut überlegten OU-Struktur ist es möglich die Administration der Domäne entscheidend zu erleichtern und dementsprechend übersichtlich zu gestalten.

Die Definition von OUs kann grundsätzlich aus 3 Gründen erfolgen:

- Delegation von Verwaltungsaufgaben
- Verwaltung von Gruppenrichtlinien
- Ausblendung von Objekten

Im Fall der Firma Buntmetall Amstetten GmbH kommt ausschließlich der Punkt Verwaltung von Gruppenrichtlinien zu tragen. Der Punkt Ausblendung von Objekten kann aufgrund des Nicht-Erfordernisses außer Acht gelassen werden. Ebenso der Punkt Delegation von Verwaltungsaufgaben, da aufgrund der Größe der Organisation eine zentralisierte Verwaltung der Infrastruktur erfolgt und die Weitergabe von Verwaltungsaufgaben nicht erforderlich ist.

Bevor eine angemessene OU-Struktur zur Verwaltung von Gruppenrichtlinien entworfen und implementiert werden kann, gilt es die Anforderungen für unterschiedliche Gruppenrichtlinien zu erkennen. Dabei müssen diverse Aspekte wie z.B. unterschiedliche Betriebssysteme, Funktion des Computers (Server od. Client), Unterscheidung zwischen Benutzer- und Computerkonten des Verwaltungsbereiches bzw. des Produktionsbereiches des Unternehmens, abweichende Anforderungen in den verschiedenen Abteilungen, etc. berücksichtigt werden.

9.2 Gruppenrichtlinien

Gruppenrichtlinien bieten dem Administrator der Domäne eine enorme Anzahl von Konfigurations- bzw. Eingriffmöglichkeiten in die Verwaltung von Benutzer- und Computerkonten. Diese können auf folgende Objekte angewandt werden:

- Standort
- Domäne
- OU

Bei der Firma Buntmetall Amstetten GmbH kommt hierbei lediglich die Möglichkeit der Anwendung von Gruppenrichtlinien auf OUs in Frage, da aufgrund der Größe des Unternehmens keine weiteren Domänen in der Gesamtstruktur enthalten sind und des weiteren nur ein Standort existiert.

Für die Erstellung einer effizienten Gruppenrichtlinienstrategie müssen vorab die unterschiedlichen Anforderungen an die jeweiligen Benutzer bzw. Computer definiert werden.

9.3 Remote-Desktops

Mit der Migration zu Microsoft Windows 2003 wurde die komfortable Nutzung von Remote-Desktops zur Verwaltung diverser Server ermöglicht. Da bei der Firma Buntmetall Amstetten GmbH in der aktuellen Umgebung alternative Fernwartungswerkzeuge im Einsatz sind, sollte hier eine Analyse durchgeführt werden, welche die Vor- bzw. Nachteile der integrierten Fernwartungsmöglichkeiten der neuen Betriebssysteme im Vergleich zur Weiterverwendung der alternativen Fernwartungstools aufzeigt.

Da diese alternativen Fernwartungstools auch in der Konzernzentrale in Deutschland eingesetzt werden und von dort aus auch ein Zugriff der Administratoren auf gewisse lokale Server möglich sein soll, muss der eventuelle Ersatz der alternativen Fernwartungstools auch mit der Konzernleitung abgestimmt werden.

9.4 Terminal Services

Terminal Services bieten die Möglichkeit, dass Clients (diese werden in diesem Fall allgemein als Thin-Clients bezeichnet) ihre Aufgaben remote auf einem Server abarbeiten. Dadurch ergeben sich geringere Anforderungen an die Hardware dieser Thin-Clients. Weiters kann dadurch eine Reduzierung der Administrationskosten erreicht werden, da die erforderlichen Softwareinstallationen und Änderungen am System zentralisiert auf einem Server durchgeführt werden können.

Da bei der Firma Buntmetall Amstetten GmbH bereits an der Umstellung der Clients auf das Betriebssystem Microsoft Windows XP begonnen wurde und diese sich noch über einige Monate erstrecken wird, ist im Moment keine Änderung dieser Strategie vorstellbar.

9.5 RIS (Remote Installation Service)

Mit Hilfe dieser neuen Möglichkeit ab Windows 2000 ist es möglich, Client-Computer vollkommen unbeaufsichtigt mit einem Betriebssystem auszurüsten. Des Weiteren können in Verbindung mit Active Directory und Gruppenrichtlinien abhängig von Computer od. Benutzer Softwareinstallationen durchgeführt

werden. Somit kann erreicht werden, dass Benutzer unabhängig vom Arbeitsplatz an dem sie sich anmelden, immer auf die von ihnen benötige Software zugreifen können.

Da bei der Firma Buntmetall Amstetten GmbH und deren Konzernleitung in Deutschlang auch hier Alternativen zum Microsoft RIS Server im Einsatz sind, müssen auch hier Analysen und Tests durchgeführt werden, um die für das Unternehmen am besten geeignete Software zu erkennen.

9.6 RAS (Remote Access Service)

Das Remote Access Service ermöglicht Clients sich in das Firmennetzwerk einzuwählen. Damit entsteht für den Client die Möglichkeit auf sämtliche Ressourcen zuzugreifen, als befände er sich direkt in diesem Netzwerk.

Wie in dieser Arbeit schon des Öfteren darauf hingewiesen wurde, existiert der einzige Zugang auf das Internet seitens der Konzernleitung in Deutschland. Somit erfolgt auch die gesamte Administration von externen Zugriffen auf das konzernweite Netzwerk durch IT-Administratoren der Konzernleitung. Daher muss auch eine Einrichtung eines externen Remote Zugangs mit den verantwortlichen Administratoren der Konzernleitung abgestimmt werden. Vom momentanen Standpunkt ist allerdings bekannt, dass seitens der Konzernleitung alternative Möglichkeiten zu RAS in Verwendung sind und somit die Verwendung von RAS für den externen Zugriff im Moment nicht angestrebt wird.

10 Zusammenfassung

Zu Beginn dieser Diplomarbeit wurde eine detaillierte Analyse der bestehenden Infrastruktur der Firma Buntmetall Amstetten GmbH durchgeführt. Die dabei gewonnen Erkenntnisse und Gegebenheiten wurden im zweiten Kaptitel dieser Arbeit genau aufgegliedert und bilden die Grundlage für die darauf erfolgte Erarbeitung der Thematik der Migration der Microsoft Windows NT 4.0 Domäne in eine Microsoft Windows Server 2003 Active Directory Domäne.

In den darauf folgenden Kapiteln wurden anschließend die Möglichkeiten der Einführung von Active Directory in eine Unternehmensstruktur und die damit in Verbindung stehenden Thematiken, welche einen unmittelbaren Einfluss auf die weiterführende Planung haben, erarbeitet. Um eine Entscheidungsgrundlage zu schaffen, wurden in weiterer Folge Unternehmensziele und Erwartungen an das neue System definiert. Danach wurde eine Gegenüberstellung der Vor- bzw. Nachteile der verschiedenen Umsetzungsvarianten im Hinblick auf die zuvor festgelegten Ziele durchgeführt. Abschließend konnten aufgrund dieser gesammelten Informationen Entscheidungen bezüglich der bevorzugten Variante zur praktischen Umsetzung dieser Arbeit getroffen werden.

Nachdem sämtliche Entscheidungen, welche die Grundlage für die spätere Planung bilden, getroffen waren, wurde mit der Planung der Migration der Domäne begonnen. Hierbei erfolgten eine exakte Erfassung der vorbereitenden Maßnahmen sowie die Festlegung diverser Nachbearbeitungsaufgaben.

Im siebten Kapitel dieser Diplomarbeit wurde aufgrund der vorher geschaffenen Grundlagen ein praktischer Leitfaden für die Durchführung eines Updates der Domänencontroller und somit für die Umstellung der Domäne entworfen, welcher dem Leser als Hilfestellung für die praktische Umsetzung dienen soll.

Darauf folgend beschreibt das nächste Kapitel sämtliche Anforderungen an die Durchführung einer Migration. Hier werden auch die Auswirkungen auf bestehende Dienste und Anwendungen, welche aufgrund der Migration zu erwarten sind, aufgezeigt.

Zu guter Letzt beschreibt das abschließende Kapitel noch den Gewinn, welchen eine solche Migration für das Unternehmen mit sich bringt und welche Möglichkeiten sich dadurch für den zukünftigen Betrieb der Produktionsumgebung ergeben. Dabei wurde auf neue und verbesserte Technologien, welche aufgrund der Einführung von Active Directory und der Umstellung auf Microsoft Windows Server 2003 zur Verfügung gestellt werden, näher eingegangen.

A Literaturverzeichnis

Bücher

Microsoft (2003 a): Migration von NT Server 4.0 auf Windows Server 2003. Microsoft Press 2003

Microsoft (2003 b): Microsoft Windows Server 2003 Active Directory-Infrastruktur. Microsoft Press 2003

Microsoft (2000): Designing a Microsoft Windows 2000 Migration Strategy. Microsoft Official Curriculum 2000

Internet

Microsoft (2006 a): Aspekte mehrerer Gesamtstrukturen in Windows 2000 und Windows Server 2003
http://www.microsoft.com/germany/technet/datenbank/articles/600393.mspx
(Datum des Zugriffs: 11.04.2006)

Microsoft (2006 b): Grundlegendes zu Vertrauensstellungen
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/de/library/ServerHelp/7b075a25-9f29-4856-883c-f230a8ccd681.mspx
(Datum des Zugriffs: 10.04.2006)

Microsoft (2006 c): Windows Server 2003 - Handbuch für die Bereitstellung
http://www.microsoft.com/germany/technet/datenbank/articles/600097.mspx
(Datum des Zugriffs: 02.05.2006)

Microsoft (2006 d): Windows-Zeitdienst (Übersicht)
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/de/library/ServerHelp/187291de-06a4-41ba-ad05-f602d58a96ae.mspx?mfr=true
(Datum des Zugriffs: 29.05.2006)

Microsoft (2006 e): Domänen- und Gesamtstrukturfunktionalität
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/de/library/ServerHelp/b3674c9b-fab9-4c1e-a8f6-787126471271.mspx
(Datum des Zugriffs: 01.06.2006)

Netigator (2006 a): Die verschiedenen Typen der Vertrauensstellung
http://www.netigator.de/netigator/live/fachartikelarchiv/ha_artikel/powerslave,id,30455643,obj,WM,np,archiv,ng,,thes,.html
(Datum des Zugriff: 12.06.2006)

Wikipedia (2006 a): Multiprotocol Label Switching
http://de.wikipedia.org/wiki/MPLS
(Datum des Zugriffs: 13.04.2006)

Wikipedia (2006 b): Kerberos (Informatik)
http://de.wikipedia.org/wiki/Kerberos_%28Informatik%29
(Datum des Zugriff: 23.05.2006)

Wikipedia (2006 c): NTLM
http://de.wikipedia.org/wiki/NTLM
(Datum des Zugriff: 23.05.2006)

Wikipedia (2006 d): Network Time Protocol
http://de.wikipedia.org/wiki/Network_Time_Protocol
(Datum des Zugriff: 29.05.2006)

Wintotal (2006): Microsoft Gruppenrichtlinien nutzen Teil 1 - Einführung in Gruppenrichtlinien
http://www.wintotal.de/Artikel/gruppenrichtlinien/teil1/teil1.php
(Datum des Zugriff: 04.04.2006)

B Glossar

A

AD (Active Directory)

Der Verzeichnisdienst von Microsoft Windows 2000/2003 Server heißt Active Directory Service (ADS). Das Active Directory ordnet verschiedenen Netzwerkobjekten wie Benutzern, Computern u.a. Eigenschaften zu und verwaltet diese. Das Active Directory baut auf einer Datenbank auf, in der die Informationen über das Netzwerk wie Benutzer, Gruppen und Computer gespeichert werden. Active Directory stellt die zentrale Verwaltungseinheit aller darin befindlichen Objekte dar.

Active Directory Schema

Im Schema des Active Directorys werden die Definitionen sämtlicher in AD gespeicherter Objekte wie z.B. Benutzer, Computer, Gruppen, etc. in Form von Klassen bzw. Objektklassen festgelegt. Jede Gesamtstruktur besitzt ein einziges gemeinsames Schema, das bei Änderungen auf alle Domänencontroller repliziert wird.

B

BDC (Backup Domänencontroller)

Diesen Begriff gibt es nur unter Windows NT 4.0, da mit neueren Windows Versionen alle Domänencontroller gleichberechtigt sind. Der BDC besitzt ausschließlich eine Sicherheitskopie der User- und Anmeldeinformationen. D.h., dass Änderungen von Objekten wie User, Computer, Passwörter nicht von diesem bearbeitet werden können. Diese werden in regelmäßigen Abständen zwischen den Domänencontroller repliziert um somit alle Domänencontroller auf dem aktuellsten Stand zu halten. Bei Ausfall des PDCs kann der BDC die Aufgabe als Anmeldeserver übernehmen (Failover).

D

DHCP (Dynamic Host Configuration Protocol)

Dieses Protokoll ermöglicht unter Verwendung eines entsprechenden Servers die dynamische Zuweisung einer IP-Adresse und weiterer Konfigurationsparameter (Gateway, DNS-Server, etc.) an diverse Komponenten in einem Netzwerk. Es vereinfacht somit die Administration von größeren Netzwerken, da die Konfiguration die einem Client zugewiesen wird an zentraler Stelle, anstatt auf jedem einzelnen Client, konfiguriert werden kann. Die Clients müssen nur einmalig für den automatischen Bezug dieser Konfiguration eingestellt werden. DHCP läuft standardmäßig auf Port 67.

DNS (Domain Name System)

Das Domain Name System (DNS) ist einer der wichtigsten Dienste im Internet. DNS dient der Umsetzung von Domainnamen in IP-Adressen und umgekehrt. Es bietet somit eine Vereinfachung, da Menschen sich Namen grundsätzlich besser merken als die zugehörigen IP-Adressen. DNS läuft standardmäßig auf Port 53.

Domäne

Unter Domäne versteht man die Abgrenzung der von Active Directory verwalteten Objekte wie Benutzer, Computer, Gruppen, etc. Alle Objekte innerhalb einer Domäne befinden sich in einer Verzeichnisdatenbank und nutzen gemeinsame Sicherheitsrichtlinien. AD-Domänen dürfen nicht mit DNS-Domänen verwechselt werden, obwohl sie oftmals die gleiche Bezeichnung zugewiesen bekommen.

Dynamic DNS (DDNS)

Als Dynamic DNS wird ein DNS Dienst bezeichnet der Dynamische Updates unterstützt und somit eine automatische Anpassung der DNS Einträge zulässt.

Dynamisches Update

Mit Hilfe von dynamischen Updates ist es möglich Zonendateien eines DNS Servers zu modifizieren. Dies bietet den großen Vorteil, dass eine Änderung völlig automatisiert ablaufen kann und nicht manuell eingetragen werden muss. Dynamische Updates werden bei einem Primary/Slave Konzept eines DNS Dienstes nur vom primären DNS Server akzeptiert. Dynamische Updates werden speziell für die Verwendung von Active Directory empfohlen.

F

Forward-Lookupzone

Mit Hilfe einer Forward-Lookupzone kann die zu einem Domänen-Namen zugehörige IP-Adresse ermittelt werden.

FQDN (Fully Qualified Domain Name)

Der Fully Qualified Domain Name beschreibt einen eindeutigen Knoten im hierarchisch aufgebauten DNS. So kann zum Beispiel der Name *buntmetall* nicht eindeutig zugeordnet werden, da dieser sowohl im Zweig .de also auch im Zweig .at existieren könnte. Mit Angabe des FQDN buntmetall.at ist allerdings eine eindeutige Zuweisung möglich.

G

Gesamtstruktur

Der Zusammenschluss mehrerer Domänen unter Benutzung eines einheitlichen Schemas, einer einheitlichen Konfiguration und eines globalen Katalogs. Innerhalb einer Gesamtstruktur erfolgt die Verwaltung einer od. mehrerer Domänen. Eine Gesamtstruktur wird auch als Forest bezeichnet.

Globaler Katalog

Der globale Katalog ist ein Domänencontroller, der eine Kopie aller Active Directory-Objekte in einer Gesamtstruktur speichert. Dieser speichert ein vollständiges Replikat aller Objekte der eigenen Domäne und ein Teilreplikat aller Objekte für alle anderen Domänen in der Gesamtstruktur.

Gruppenrichtlinien

„Gruppenrichtlinien sind Sammlungen von Benutzer- und Computerkonfigurationseinstellungen, die mit Computern, Standorten, Domänen oder Organisationseinheiten (OUs) verknüpft werden, um das Verhalten des Benutzerdesktops zu steuern und darüber hinaus Dinge wie Sicherheitseinstellungen, Anmelde- und Abmeldeskripte, Skripte für den Start und das Herunterfahren eines Computers zu definieren oder z.B. Ordnerumleitungen festzulegen. Mit Gruppenrichtlinien kann das Verhalten des Be-

triebssystems bestimmt und dessen Optionen eingeschränkt werden." (Wintotal, 2006)

I

Incremental Zone Transfers (IXFR)

Der inkrementelle Zonentransfer ist ein spezielles Verfahren um Zonendateien eines DNS Dienstes zu aktualisieren. Der wesentliche Vorteil dieses Verfahrens ist es, die zu übertragende Datenmenge während einer Aktualisierung zwischen einem primären DNS Server und einem sekundären DNS Server zu minimieren, indem nur die Änderungen seit der letzten Aktualisierung übertragen werden.

K

Kerberos

„Kerberos ist ein verteilter Authentifizierungsdienst (Netzwerkprotokoll) zur Authentifizierung, der für offene und unsichere Computernetze (z. B. das Internet) von Steve Miller und Clifford Neuman entwickelt wurde. Die zurzeit aktuelle Version ist Kerberos 5. Microsoft verwendet Kerberos als Standard-Protokoll für die Authentifizierung unter Windows 2000/2003 basierten Netzwerken sowie für den Windows XP-Client." (Wikipedia, 2006 b)

M

MPLS (Multiprotokoll Label Switching)

„Beim Multiprotocol Label Switching handelt es sich um eine Implementation des Label Switching. Bei solchen Verfahren werden die am Transport eines Datenpaketes beteiligten Router stark entlastet, da sich das Komplexitätsniveau auf das eines Switches reduziert. Dies wird erzielt, indem zu Beginn der Datenübertragung ein fester Verbindungsweg eingerichtet wird. Router auf diesem Weg müssen weiterzuleitende Datenpakete nicht mehr auf ihren Empfänger untersuchen, sondern geben diese ohne weitere Bearbeitung entsprechend des zuvor geschalteten Weges weiter." (Wikipedia, 2006 a)

N

NTLM (Abk. für NT LAN Manager)

„NTLM ist ein Computer-Authentifizierungsschema und nutzt einen 4-Wege-Handshake. NTLM ist ein propriäterer Standard der Firma Microsoft und ist daher fast ausschließlich in Produkten dieses Herstellers implementiert. Aufgrund von Sicherheitproblemen wurde NTLMv2 Nachfolger von NTLM. Ein alternatives, offenes Protokoll ist Kerberos." (Wikipedia, 2006 c)

NTP (Network Time Protocol)

„Das Network Time Protocol (NTP) ist ein Standard zur Synchronisierung von Uhren in Computersystemen über paketbasierte Kommunikationsnetze. Obwohl es meistens über UDP abgewickelt wird, kann es durchaus auch über andere Layer-4-Protokolle wie z.B. TCP transportiert werden. Es wurde speziell dafür entwickelt, eine zuverlässige Zeitgabe über Netzwerke mit variabler Paketlaufzeit (Ping) zu ermöglichen." (Wikipedia, 2006 d)

P

PDC (Primary Domänencontroller)

PDC ist ebenfalls ein Begriff aus Windows NT 4.0 Domänen. Es kann in jeder Domäne nur einen Domänencontroller geben, der als solcher definiert ist. Weiters ist es ausschließlich dem PDC vorbehalten diverse Änderungen von Objekten einer Domäne zu verarbeiten.

R

Reverse-Lookupzone

Mit Hilfe einer Reverse-Lookupzone kann im Gegensatz zu einer Forward-Lookupzone der zu einer IP-Adresse zugehörige Domänen-Name ermittelt werden. Solche Anfragen werden als inverse Anfragen bezeichnet. Um dies zu ermöglichen wurde eine eigene Domäne mit der Bezeichnung in-addr.arpa entworfen. Die Domäne 10.131.in-addr.arpa. enthält damit die IP-Adressen 10.131.x.y.

S

SRV Resource Records

Mit Hilfe von SRV Resource Records können Dienste, welche auf dem Internet Protokoll basieren, in einer Domäne lokalisiert werden. Durch Abfragen dieser Dienste erhält man Informationen wie z.B. den Server der diesen Dienst zur Verfügung stellt. Für die Darstellung werden dazu Unterstriche verwendet. Zuerst erfolgt dabei die Angabe des Dienstes gefolgt vom verwendeten Protokoll.
Beispiel: _ldap._tcp.example.com

Stammdomäne (Root-Domäne)

Im Active Directory wird die erste Domäne einer neuen Gesamtstruktur als Stammdomäne bezeichnet. Unterhalb dieser Domänen können dann Subdomänen für Unternehmensbereiche, Abteilungen, etc. erstellt werden. Die Stammdomäne einer Active Directory Gesamstruktur darf allerdings nicht mit der Stammdomäne des DNS verwechselt werden. Die Stammdomäne in AD kann somit auch den Name*n intern.buntmetall.at* haben, wohingegen die Stammdomäne des DNS immer der . ist.

Subdomäne

Als Subdomäne werden jene Domänen bezeichnet die unterhalb einer anderen Domäne liegen. So könnte zum Beispiel die Domäne *test.buntmetall.at* eine Subdomäne von *buntmetall.at* sein. Speziell in Active Directory werden Subdomänen immer unterhalb der Stammdomäne erzeugt. Subdomänen können aber natürlich auch ineinander verschachtelt erstellt werden.

Systemrichtlinien

Mit Hilfe von Systemrichtlinien ist es möglich, den Benutzer hinsichtlich der Einflussnahme auf die Systemumgebung einzuschränken. Systemrichtlinien kommen in Windows NT 4.0 Domänen zum Einsatz und wurden mit Microsoft Windows von Gruppenrichtlinien abgelöst. Ein wesentlicher Unterschied ist, dass Systemrichtlinien permanent in die Registrierung geschrieben werden und erst durch eine gegenteilige Einstellung wieder aufgehoben werden. Dieses Verhalten wird auch als „Tatooing" bezeichnet. Bei Gruppenrichtlinien hingegen erfolgt keine dauerhafte Einbettung der Vorgaben in die Registrierung. Die Vorgabe kann somit einfach durch Aufheben der Gruppenrichtlinie rückgängig gemacht werden.

V

Vertrauensstellung

Eine Vertrauensstellung schafft die Möglichkeit der Authentifizierung und des Zugriffs auf Ressourcen in zwei nicht zusammenhängenden Domänen. Damit ist es möglich, dass Benutzer einer Domäne in einer anderen Domäne authentifiziert werden und somit lokale Ressourcen der anderen Domäne nutzen können. Dabei gibt es verschiedene Arten von Vertrauensstellungen. Unter Windows Server 2003 wird bei der Erstellung einer neuen Domäne einer Gesamtstruktur automatisch eine Vertrauensstellung mit der übergeordneten Domäne erstellt.

W

WINS (Windows Internet Naming Service)

WINS ist in seiner Funktionalität dem DNS sehr ähnlich und bietet auch wie DNS die Möglichkeit für dynamische Aktualisierungen. Dabei registriert ein Host während dem Startprozess seinen Namen automatisch am WINS-Server. Zusätzlich zum NetBIOS-Namen des Rechners werden auch Namen wie jener der Domäne bzw. Arbeitsgruppe, angemeldete Benutzer, Benutzergruppen, Domänencontroller, etc. am WINS-Server registriert. Ab Windows 2000 hat sich Microsoft allerdings von dieser Technologie entfernt und der Verwendung von DNS zugewandt.

Z

Zonentransfer (auch Zonenübertragung)

Der Zonentransfer stellt wie auch der inkrementelle Zonentransfer ein Verfahren zur Aktualisierung von Zonendateien eines DNS Dienstes dar. Dabei werden aber stets die vollständigen Zonendaten übertragen. Dies stellte natürlich eine wesentlich höhere Netzwerkbelastung dar und kommt vor allem in älteren Implementierungen von DNS Diensten, welche noch keine Unterstützung für Incremental Zone Transfers bieten, zur Anwendung.

C Abbildungsverzeichnis

D Tabellenverzeichnis