

Inhaltsverzeichnis:

1	Einleitung	2
1.1	Vorstellung des Ausbildungsbetriebs.....	2
1.2	Beschreibung des Aufgabenbereiches	2
1.3	Thema der Projektarbeit.....	2
2	Projektplan	3
3	Analyse des Ist-Zustandes	3
4	Soll Zustand	4
5	Lösungskonzept	4
5.1	Gliederung des Projektablaufes	4
6	Realisierung	4
6.1	Konfiguration vorhandener Server.....	4
6.2	Vorüberlegung:	5
7	Installation der Server	5
8	Konfiguration der Server	6
8.1	Einrichten der Windows 2003 Active Directory Domäne	6
8.2	Einrichten des DNS Servers.....	6
8.3	DNS Zonentypen	7
8.4	Einrichten des DHCP Servers	7
8.5	Einführung in WSUS	7
8.6	Installation von WSUS	8
8.7	Vor- und Nachteile von WSUS	8
8.8	Erstellen der Leistungs- und Auditing Monitore.....	9
8.9	Warum werden diese 3 Punkte überwacht?	9
8.10	Welche Leistungsindikatoren werden für welche Komponente erstellt	9
8.11	Erstellen einer Überwachungsrichtlinie auf Dateien, Ordner und Freigaben	10
8.12	Die Domänenfunktionsebenen	10
9	Installation / Konfiguration der Clientcomputer	11
9.1	Konfiguration von WSUS an den Clients	11
9.2	Einrichten der Freigaben nach Kundenwunsch.....	12
9.3	Einschränken der Benutzer mittels Gruppenrichtlinien.....	12
9.4	Warum Gruppenrichtlinien?.....	13
9.5	Wo werden Gruppenrichtlinien eingesetzt?	13
9.6	Erstellen der Benutzerprofile	14
9.7	Bereitgestellte Ressourcen per Script bereitstellen.....	14
10	Sicherungstechnische Maßnahmen	15
11	Test des EDV Systems	15
12	Übergabe und Einführung der Mitarbeiter in das neue System	16
13	Fazit / Ausblick	16
	Anhang	
	Glossar	
	Quellenangaben	
	Erklärung zur betrieblichen Projektarbeit	

1 Einleitung

Zu Beginn der Dokumentation meiner Projektarbeit beschreibe ich kurz meinen Ausbildungsbetrieb und die Aufgaben im Projekt.

1.1 *Vorstellung des Ausbildungsbetriebs*

1994 Gründung als Einzelunternehmen (keine Mitarbeiter)

1996 Umzug von Tiefenbach nach Schönberg und damit Start des Großhandelsgeschäftes mit 3 Mitarbeitern

1999 14 Mitarbeiter

2003 19 Mitarbeiter

2006 34 Mitarbeiter

2007 40 Mitarbeiter

Die Witter GmbH bietet dem Handel attraktive Produkte für das Sortiments- und Aktionsgeschäft. Logistik- und After-Sales-Service werden kundenorientiert optimiert wahrgenommen.

Die Witter GmbH ist spezialisiert auf Elektronikprodukte - insbesondere für die Produktbereiche Computertechnik, Telekommunikation, Haushaltsgeräte und Unterhaltungselektronik. Die Produkte erfüllen hinsichtlich Qualität und Preis-Leistungs-Verhältnis alle Voraussetzungen, um Sortimentsgeschäft und Verkaufsaktionen zum Erfolg zu führen.

1.2 *Beschreibung des Aufgabenbereiches*

Um mögliche Ausfallzeiten in unserer Firma gering zu halten, gehört die Wartung und Instandhaltung, Überwachung und Konfiguration des Netzwerks zu meinem Tätigkeitsumfeld. Um Sicherheitsrisiken im Netzwerk frühzeitig zu erkennen und zu beheben gehört die Patchverteilung mittels WSUS ebenfalls dazu. Die Pflege und Aktualisierung der vorhandenen Dokumentationen gehört zu meinem Aufgabenbereich.

1.3 *Thema der Projektarbeit*

Das Thema der Projektarbeit lautet: „Erstellung einer Windows 2003 Domäne inklusive Rechtevergabe und automatische Updateverteilung“. Dazu gehört das Erarbeiten eines geeigneten Projektablaufs. Nach dem Gespräch mit dem Niederlassungsleiter des Kunden in der Zweigstelle in Dessau erfolgt eine Durchführung einer Ist-Analyse und eines Soll-Konzepts. Diese Abläufe helfen mir bei der Projektdurchführung, ferner kann noch eine Kostenaufstellung für die Zweigstelle durchgeführt werden. In der Zweigstelle sollten längere Systemausfälle vermieden werden. Um die Netzwerkverwaltung firmenintern identisch zu gestalten, soll die bisherige Linux-Lösung abgeschafft und durch ein identisch strukturiertes Windows 2003 Active Directory ersetzt werden, da die bisherigen Linux-Administratoren im Zuge der Firmenübernahme die Niederlassung in Dessau verlassen haben. Der Name der Firma wurde hierbei für die Projektdokumentation auf expliziten Wunsch nach XYZ.local abgeändert.

2 Projektplan

Tabelle des Projektablaufs

Meinen Projektablauf plane ich wie folgt:

Projektschritte	Geplante Dauer in Stunden
Durchführung einer Ist-Analyse	1
Erarbeitung eines Soll-Konzepts	3
Installation der Server	5
Konfiguration der Server	8
Erstellen und verteilen der Clientimages	4
Installation / Konfiguration von WSUS	2
Erstellen der Anmeldescripts per Batch	1
Erstellen der Leistungs- Auditing Monitore	3
Erstellen der Benutzer und Freigaben	5
Schulung der Benutzer	3
Gesamtaufwand	35

3 Analyse des Ist-Zustandes

Wie schon im Projektantrag beschrieben wurde, wird im Rahmen des Projekts das komplette Netzwerk der Zweigstelle in Dessau umstrukturiert. Dadurch dass es in unserem Unternehmen keinen Administrator mit fundierten Linux-Kenntnissen gibt, wird das bisherige Linux-System nach Windows 2003 Active Directory migriert. Leider war das bisherige System weder ausreichend dokumentiert noch ausfallsicher gestaltet. Aus diesem Grund entschied sich die Firmenleitung für den Aufbau einer identischen AD-Struktur in der Niederlassung analog zur Zentrale. In der Zweigstelle sind Client-PCs vorhanden, die ohne Probleme weiter verwendet werden können (HP Compaq EVO D510, 2,4 GHz, 1GB RAM, 40GB HDD). Da es versäumt wurde eine strukturierte Rechtevergabe einzuführen, hat sich im Laufe der Zeit einiges an überflüssigen Daten angesammelt. Diese Daten werden von Mitarbeitern aussortiert, damit nach der Datenübernahme auf das neue System Ordnung herrscht. Der alte Server in der Zweigstelle wird ebenfalls ausgemustert und durch zwei HP DL360 G3 ersetzt, die in der Hauptstelle in Schönberg im Moment nicht gebraucht werden.

In der Zweigstelle in Dessau waren die Netzwerkkomponenten schon vorhanden. Ein HP 2650 Switch mit 48 10/100 Mbit Ports und 2 1000 Mbit Ports. Der bisherige Linux-Server war leider nur über einen 100MBit/s Uplink am Netz angebunden.

4 Soll-Zustand

Nach der Umsetzung des Projekts in der Zweigstelle sollen die Netzwerkdienste, wie DNS, Active Directory und WINS redundant laufen, damit das Netzwerk ausfallsicherer wird. Außerdem sollten die verschiedenen Abteilungen im Active Directory mit Hilfe OUs abgebildet werden, damit durch Gruppenrichtlinien einfacher Sicherheitsrichtlinien umgesetzt werden können. Damit die Clients in der Niederlassung Dessau auf dem Laufenden gehalten werden, wird ein WSUS implementiert um die Updateverteilung gleichmäßig durchführen zu können. Ein weiterer wichtiger Punkt war, die Gesamtkosten auf Dauer zu senken, da bei der vorhandenen Linux-Lösung die Kosten durch den Administrationsaufwand fast jährlich gestiegen sind. Wenn in der Zweigstelle in Dessau im Laufe der Zeit ein schnellerer DSL-Anschluss größer 384 kbit/s zur Verfügung steht, soll die Zweigstelle an die Hauptstelle mittels VPN dauerhaft angebunden werden (im Augenblick wird eine VPN-Verbindung nur für administrative Zwecke aufgebaut). Nach erfolgreichem Projektabschluss wird eine übersichtliche Domänenstruktur vorhanden sein, die sich zum einen an offene Standards hält und zum anderen viel leichter von den Administratoren zu pflegen ist. (siehe Anhang [A1])

5 Lösungskonzept

Um einen reibungslosen Projektablauf zu gewährleisten, habe ich mein Projekt in folgende Punkte gegliedert.

5.1 Gliederung des Projektablaufes

Teilbereiche

- | Vorüberlegungen zur Installation
- | Installation der Server
- | Konfiguration der Server
- | Installation der Clients und erstellen eines Images für die Clients
- | Verteilung der Images an die Clients
- | Installation von WSUS
- | Erstellen der Gruppenrichtlinie für WSUS
- | Erstellen des Loginscripts
- | Erstellen der dynamischen servergespeicherten Profile

6 Realisierung

Dadurch dass der Server in der Zweigstelle schon relativ alt ist, werde ich diesen durch zwei HP DL 360 G3 ersetzen. Da in der Hauptstelle noch zwei HP DL 360 zur Verfügung stehen, können diese in der Nebenstelle in Dessau eingesetzt werden. Diese beiden Server sind in der Hauptstelle bei einem Projekt übrig geblieben und können in der Zweigstelle in Dessau sinnvoll eingesetzt werden.

6.1 Konfiguration vorhandener Server

Es sind zwei HP DL 360 G3 vorhanden:

Server 1:

- | DL 360 G3
- | 2x 146 GB SCSI Festplatte 10000 U/Min.
- | 2x 1024 MB Ram ECC Reg.
- | Raidkonfiguration Raid 1 (Spiegelung)
- | Raidcontroller Onboard HP Smart Array 5i

- | Ultra SCSI 320 SCSI adapter
- | 2x NC 7781 PCI-X Gigabit NIC
- | 2x 400 W Netzteil Hotplug

Server 2:

- | DL 360 G3
- | 2x 72 GB SCSI Festplatte 10000 U/Min.
- | 2x 1024 MB Ram ECC Reg.
- | Raidkonfiguration Raid 1 (Spiegelung)
- | Raidcontroller Onboard HP Smart Array 5i
- | 2x NC 7781 PCI-X Gigabit NIC
- | 2x 400 W Netzteil Hotplug

6.2 Vorüberlegung:

Bevor ich mit dem Projekt begann, wurde zum einen erst besprochen, welche Anforderungen an das Netzwerk gestellt werden. Dabei spielte der Punkt Lastenverteilung eine sehr große Rolle. In den Servern wird ein Raid-System mit dem Raidlevel 1 eingerichtet, um sich vor einem Systemausfall durch Festplattenschaden zu schützen. Redundante Netzteile sind auch mit eingebaut, um das System vor einem Netzteildefekt abzusichern. Auf beiden Servern werden zwei Partitionen eingerichtet, die erste Partition mit 30 GB für das Betriebssystem und die zweite für Daten. Auf Server 2 wird die zweite Partition für Windowsupdates von WSUS verwendet. Zusätzlich wird auf Server 2 noch Symantec Norton Ghost installiert und die Images der Clients auf der zweiten Partition abgelegt. Server 1 mit den zwei 146 GB SCSI Platten wird zum Fileserver und zum Domainmaster in der Domäne XYZ, Server 2 wird auch Domänencontroller. Auf dem zweiten Server wird Windows Server Update Service installiert und die WSUS Updates lokal auf dem Server gespeichert. Ein großer Vorteil gegenüber einer Lösung ohne WSUS ist, dass die Sicherheitsupdates nur ein Mal vom Internet herunter geladen werden müssen. Mit dieser Lösung spart man sich erstens Internettraffic und der administrative Aufwand sinkt. Mit Hilfe von Mitarbeitern aus den verschiedenen Abteilungen wird eine Liste aller benötigten Programme für das Image der Clients erarbeitet. In der Niederlassung in Dessau läuft natürlich auch ein DNS, WINS und DHCP Server, diese Dienste werden auf beiden Servern implementiert, um nach einem Servercrash immer noch im Netzwerk weiterarbeiten zu können. Da DHCP keine echte Funktion besitzt, um einen einzigen Bereich redundant zu erstellen, lege ich auf beiden Servern einen sich nicht überschneidenden DHCP-Pool an. Bei der automatischen IP-Adressverteilung vergibt der schnellere DHCP im Netzwerk die IP-Adresse, Subnetzmaske, DNS Server und Default Gateway. Die Firmenstruktur soll im Active Directory abgebildet werden und ist deshalb in verschiedene OUs unterteilt.

7 Installation der Server

Bevor der alte Linux-Server außer Betrieb genommen wird, müssen erst einmal die alten Datenbestände weggesichert werden. Diese Daten werden vorübergehend auf eine Adminworkstation kopiert. Da die Lizenzen für die Server noch nicht vorhanden sind, habe ich dem Geschäftsführer der Zweigstelle empfohlen zwei Windows Server 2003 R2 Standard Lizenzen zu besorgen, da diese für die Anforderungen in Dessau zum einen ausreichend, zum anderen kostengünstiger als z.B. die Enterprise Version sind (dieser Funktionsumfang wird nicht benötigt).

Bei der Installation der beiden HP DL 360 gehe ich wie folgt vor: Bei den HP Proliant Servern wird die Raidkonfiguration und die Grundinstallation mit Hilfe der HP Smart

Start Software durchgeführt. In diesem Setup kann das Raid-Array konfiguriert werden. Da in den Servern nur zwei Platten vorhanden sind, stehen nur die Raid-Level 0 und 1 zur Auswahl. Nach der Grundkonfiguration des Servers kann man mit der Software auswählen, welches Betriebssystem installiert werden soll. Dieser Vorgang ähnelt dann einer Grundinstallation von Windows. Ein weiterer Vorteil bei der Installation der Server mit der HP Smart Start Software ist, dass alle benötigten Treiber beim ersten Hochfahren installiert werden. Jetzt muss das System nur noch upgedatet werden, und dann kann mit der Konfiguration begonnen werden.

8 Konfiguration der Server

Nachdem die Server installiert sind, werden alle aktuellen Sicherheitspatches eingepielt. Bevor mit der Installation von Active Directory begonnen wird, sollten ein eindeutiger Computernamen sowie fixe IP-Adressen vergeben sein. (Anhang [A2] Domänenstruktur)

8.1 Einrichten der Windows 2003 Active Directory Domäne

Der erste Schritt in der Installation von Active Directory ist, dass man Server 1 zum Domänencontroller heraufstuft. Damit die gewünschte Redundanz im Active Directory gegeben ist, wird Server 2 ebenfalls zum Domänencontroller promotet. Ein Domain Controller hat folgende Rollen im Netzwerk.

FSMO (Flexible Single Master Operation) – Rollen

1. Schema Master

- Ist für den Aufbau im AD zuständig
- Einmalig in einer kompletten AD Umgebung

2. RID- Master

- Sorgt für eindeutige Identifizierung von Objekten im AD in jeder Domäne
- Pro Domäne einmal vorhanden

3. Domänennamenmaster (DNS-Master)

- Sorgt für eindeutige Namensvergabe im Forest

4. Infrastrukturmater diese Rolle wird auf den zweiten AD Controller verschoben

- Verfolgung über Informationen von Objekten in der Domäne
- Pro Domäne einmal vorhanden
- Z.B. Verschieben einer OU, Änderung von Gruppeneigenschaften
- Ist für die Aktualisierung des Global Katalog Servers zuständig

5. PDC – Emulator

- Abwärtskompatibilität für Windows NT
- Zuständig für die Benutzerpasswörter

Nachdem die Domänencontroller installiert wurden, konnte mit der Einrichtung von Active Directory begonnen werden. Da dies schon im Vorfeld besprochen wurde, verlief die Einrichtung problemlos.

8.2 Einrichten des DNS Servers

Der Zweck einer DNS-Lösung besteht darin, dass die Benutzer auf die Daten mittels einfacher Namen gelangen. Beim Anmelden an einer Domäne fragt der Client beim DNS Server den Namen des AD-Controllers und des Kerberos Dienstes nach (SRV Ressourceneinträge). Sowohl DNS Clients als auch Server führen Abfragen zur Namensauflösung durch. DNS bildet sowohl die Grundlage des Internet-

Benennungsschemas als auch des Active Directory-Domänen-Benennungsschemas einer Organisation. DNS unterstützt den Zugriff auf Ressourcen über alphanumerische Namen. Ohne DNS wäre es für den Zugriff auf Ressourcen erforderlich die IP Adressen der jeweiligen Ressourcen zu ermitteln. Ein DNS Server beinhaltet jeweils zwei Zonen, um Namen in IP Adressen und IP-Adressen in Namen auflösen zu können. Diese Zonen werden Forward-Lookup Namen in IP, Reverse Lookup IP in Namen genannt. Diese werden ebenfalls als AD integrierte Zonen erstellt. Eine Active Directory integrierte Zone ist eine Zone die in der Active Directory Datenbank gespeichert wird. Ein Vorteil dieser Zonen ist, dass es nicht nur einen DNS-Master, sondern mehrere geben kann. In der Zweigstelle in Dessau können z.B. auf beiden DNS-Servern Änderungen durchgeführt werden. Ein DNS-Domänenname oder FQDN (Fully Qualified Domain Name) ist wie folgt aufgebaut: Clientcomputer1.xyz.local. In einem DNS Domänennamen sind folgende Zeichen gültig: A-Z, a-z, 0-9 und der Bindestrich(-). Jeder Client führt sichere dynamische Aktualisierungen durch, bei diesem Vorgang muss sich der Client jedoch am Server authentifizieren. Diese Aktualisierungen funktionieren aber nur, wenn Active Directory integrierte Zonen vorhanden sind. Diese sicheren Aktualisierungen schützen die DNS Zone vor Fremdeingriffen. Ein DNS-Server ist je nach Anwendungsbereich anders zu konfigurieren. Er kann mehrere Zonen hosten oder wie in unserem Fall nur eine Primäre Forward Lookup und eine Primäre Reserve Lookup Zone. (Anhang [B] DNS)

8.3 DNS-Zonentypen

DNS Zonen	Beschreibung
Primäre Zone	In ihr können Ressourceneinträge erstellt und verwaltet werden
Sekundäre Zone	Ist eine schreibgeschützte Kopie einer Primären Zone
Stub Zone	Stubzonen sind Kopien einer Zone die nur die wichtigsten Ressourceneinträge erhalten, z.B. SOA, Namensserver, Host Einträge

8.4 Einrichten des DHCP Servers

Um nicht bei jedem Client eine manuelle IP-Adresse vergeben zu müssen, wird in der Zweigstelle ein DHCP-Server eingerichtet. Mit einem DHCP Server lassen sich auch viele weitere Parameter automatisch an die Clients vergeben, wie z.B. welche IP hat der Router, DNS-Domänenname, WINS Server und Knotentyp, DNS-Server und statische Routen. Um sicherzustellen, dass, eine gewisse Redundanz beim DHCP-Dienst gegeben ist, wird auf beiden Servern der DHCP Dienst installiert und so konfiguriert, dass jeder der beiden DHCP Server einen anderen IP - Adressbereich verteilt. Mit diesem kleinen Trick wird die gewünschte Redundanz in der Zweigstelle gegeben. Als weiteren Aspekt für die Lastenverteilung, wird von jedem Server der eigene DNS und WINS Server als erstes zugeteilt, dadurch werden die Rollen im normalen Netzwerkbetrieb schon einwandfrei verteilt. (Anhang [C] DHCP)

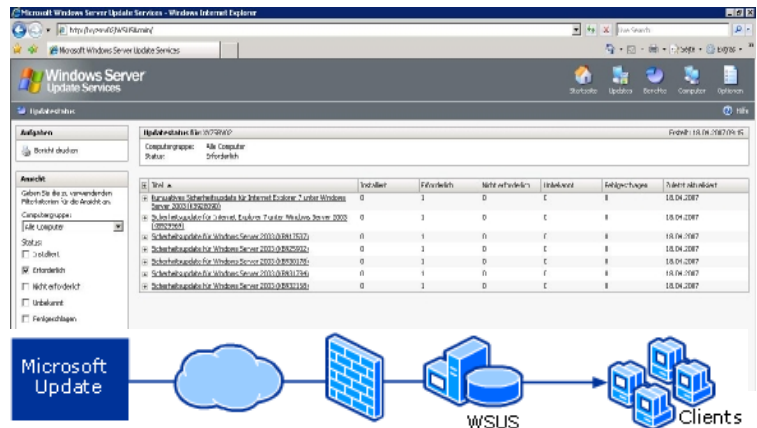
8.5 Einführung in WSUS

Bei den Windows Server Update Services (WSUS) handelt es sich um eine Patch- und Updatesoftware von Microsoft, bestehend aus einer Server- und einer Clientkomponente. WSUS unterstützt die Administratoren Microsoft-Updates in großen lokalen Netzwerken. Er lädt Update-Pakete aus dem Internet (Microsoft Update) und bietet sie den Windows-Clients zur Installation an. Der WSUS-Administrator kann am Server festlegen, welche Computer welche Updates installieren sollen. Microsoft stellt die Windows Server Update Services kostenlos zur Verfügung.

Die Serverkomponente wird auf einem Computer installiert, der unter einem Windows 2000 Server mit mindestens SP3 oder Windows Server 2003-Betriebssystem läuft. WSUS stellt Features zur Verfügung, die der Administrator benötigt um Updates über ein webbasiertes Tool zu verwalten. Darüber hinaus kann der erste WSUS-Server als Updatequelle für andere WSUS Server im Netzwerk dienen.

WSUS wird komplett über ein Web Frontend konfiguriert.

Für WSUS müssen keine Extra Prots freigegeben werden, da der WSUS-Server seine Updates über Port 80 abholt.



8.6 Installation von WSUS

Voraussetzungen:

WSUS an sich ist eine kostenlose Lösung von Microsoft, aber die Zugriffslizenzen von den Clients zum WSUS Server müssen vorhanden sein.

1 GB Speicher auf der Systempartition (C:) für WSUS

2 GB Speicher auf der Systempartition (C:) für SQL Desktop Engines die WSUS mitinstalliert. Eine weitere Partition mit Mindestens 6 GB muss vorhanden sein um die Updates Lokal auf dem Server zu speichern. Außerdem muss mindestens der Internet Information Server in Version 5.0 und das .NET Framework 1.1 auf dem WSUS Server installiert sein.

8.7 Vor- und Nachteile von WSUS

Vorteile von WSUS :

- Kostenlos
- Gute und Leichte Integration in Windows Netzwerke
- Relativ einfache Installation
- Übersichtliches Patchmanagement
- Benötigt keine zusätzlichen Ports

Nachteile von WSUS:

- Keine Unterstützung für andere Betriebssysteme (Novell oder Linux)
- Es können nur Patches von Microsoft verteilt werden, keine eigenen
- Updates liegen auf einem Server in der Firma

Voraussetzungen am Client:

- Windows 2000 Professional/Server mit mindestens SP3
- Windows XP mit mindestens SP1
- Windows 2003 Server
- Windows Vista
- Der Automatische Update Dienst muss gestartet sein

Einsatzszenario von WSUS:

- Kleinen – großen Betrieben, in denen viel von Microsoft läuft
- Testumgebungen (z.B. bevor die Updates in der Produktivumgebung freigegeben werden)

8.8 Erstellen der Leistungs- und Auditing Monitore

Um für das Netzwerk der Nebenstelle gewährleisten zu können, dass die Server jederzeit effizient und zuverlässig funktionieren, überwachen wir die Netzwerkauslastung und Hardwareauslastung vom ersten Tag an. Diese Überwachungsrichtlinien helfen uns stets bei der Optimierung des Systems. Da auch auf die Auslastung der Hardware geachtet werden sollte, werden folgende Leistungsindikatoren im System der Zweigstelle implementiert.

- Überwachen des Prozessorauslastung
- Überwachen der Datenträger
- Überwachen der RAM / Arbeitsspeicher

8.9 Warum werden diese 3 Punkte überwacht?

Der Prozessor wird bei fast allen Vorgängen auf dem Server genutzt. Im Allgemeinen sind Prozessoren von Anwendungs-Servern stärker ausgelastet als ein Backupserver, der nur nachts tätig ist. Die zwei häufigsten Ursachen bei Prozessorproblemen sind schlecht programmierte Anwendungen oder Gerätetreiber, die die CPU sehr stark auslasten. Die Datenträger im Server sind für das Speichern, Verschieben und Löschen von Daten zuständig. Dadurch haben sie einen großen Einfluss auf die Gesamtleistung des Systems. In der heutigen Zeit kann es auch immer schneller zu einer Arbeitsspeicherauslastung kommen, da die Applikationen immer anspruchsvoller werden. Um den Arbeitsspeicher besser zu überwachen, werden hier ebenfalls Leistungsindikatoren erstellt.

8.10 Welche Leistungsindikatoren werden für welche Komponente erstellt?

Prozessor:

- *System Prozessor Warteschlange*
 - Anzahl der Anfragen an die CPU, wenn dieser Wert über 10 Anfragen ist sollte man sich die Prozesse, die auf dem System laufen einmal genauer anschauen und überflüssige beenden!
- *Prozessorzeit (%)*
 - Gibt die Zeit an, in der die CPU ausgelastet ist, wenn diese Auslastung ständig über 85% liegt, wird dies als Prozessorengepass gewertet und die CPU sollte gewechselt (aufgerüstet) oder der Server entlastet werden.

Datenträger:

- *Zeit(%)*
 - Dieser Wert zeigt, wie stark der Datenträger ausgelastet wird, liegt dieser ständig über 50% sollte man überprüfen, welche Anwendung diese hohe Auslastung verursacht, und versuchen den Datenträger zu entlasten. Wenn diese Maßnahmen nichts helfen, sollte man den alten Datenträger durch einen neuen schnelleren ersetzen.
- *Bytes/s*
 - Dieser Leistungsindikator zeigt an, wie stark die Platte arbeitet. Je höher dieser Mittelwert ist, desto stärker ist die Festplatte ausgelastet.

RAM / Arbeitsspeicher:

- *Seitenfehler/s*

- Ist der Wert „Seitenfehler/s“ im Leistungsmonitor ständig über 5 Seitenfehler pro Sekunde, sollte man den Arbeitsspeicher entweder entlasten oder dem Server mehr Arbeitsspeicher hinzufügen
- *Verfügbares Bytes*
 - Ist weniger als 5% des gesamten Speichers frei, sollte man entweder mehr Arbeitsspeicher hinzufügen oder den Server entlasten.

8.11 Erstellen einer Überwachungsrichtlinie auf Dateien, Ordner und Freigaben

In der bisherigen Linux-Lösung in der Zweigstelle waren keine Überwachungsrichtlinien eingerichtet, wodurch es nach einem Systemfehler äußerst schwierig war, den Fehler nachvollziehen oder beheben zu können. Diese Probleme sollten in der neuen Lösung nicht mehr auftreten, deshalb werden geeignete Überwachungsrichtlinien auf Dateien und Ordner erstellt. Um Systemfehler schnell und effizient zu beheben, kann in der neuen Ereignisanzeige der neuen Windows Lösung überprüft werden, wer oder was diesen Fehler verursacht hat. Durch die neue Rechtevergabe in der Zweigstelle wird es den Benutzern erschwert Dateien oder Ordner zu löschen. Mit diesen Maßnahmen, kann nachgesehen werden, wer diesen Fehler verursacht hat.

8.12 Die Domänenfunktionsebenen

Damit die verschiedenen Domänencontroller untereinander kommunizieren können, werden Domänenfunktionsebenen benötigt. Dadurch dass unsere Domäne in der Niederlassung in Dessau neu aufgebaut wurde, wurde sie auf die Funktionsebene „Windows 2003“ gestuft.

Was ist eine Domänenfunktionsebene?

In der Domänenfunktionsebene wird definiert, was in der gesamten Domäne gilt. Die Domänenfunktionsebene kann je nach Umgebung heraufgestuft werden. Domänenfunktionsebenen bestimmen auch, welche Gruppeneigenschaften in der Domäne zur Verfügung stehen.

Die drei Domänenfunktionsebenen

Windows 2000 gemischt (ist Standard Funktionsebene nach einer Neuinstallation)

Unterstützt alle älteren Domänen wie z.B. Windows NT4.0 Windows 2000, hat aber den großen Nachteil, dass sie nur Globale Gruppen und Domänenlokale Gruppen unterstützt. Unterstützte Domänencontroller: Windows NT 4.0, Windows 2000 und Windows 2003.

Windows 2000 Pur

Unterstützte Domänencontroller: Windows 2000, Windows Server 2003. Funktionen: Verschachtelung von Gruppen, universelle Gruppen. Das Heraufstufen der Domänenfunktionsebene ist ohne Probleme möglich.

Windows 2003

Es werden nur noch Windows 2003 Domänencontroller unterstützt. Nach dem Heraufstufen der Domäne können keine älteren Domänencontroller, z.B. Windows 2000 in die Domäne aufgenommen werden. Unterstützte Funktionen: Umbenennen von Domänencontrollern, Aktualisierung und Replikation des Anmeldezeitstempel-Attributs. Unterstützung des Benutzerkennworts für die Objektklasse "InetOrgPerson". Erzwungene Delegation, Umleitung der Container "Benutzer" und "Computer".

9 Installation / Konfiguration der Clientcomputer

Die Installation von Windows XP Professional erfolgt gemäß dem Standardschema einer Betriebssysteminstallation, in der es keinerlei Probleme gegeben hat. Nach der Installation des Betriebssystems habe ich alle aktuellen Treiber installiert und den Rechner komplett neu upgedatet, um auf dem neusten Stand zu sein. Danach habe ich den Computer in die Domäne eingebunden und zum Abschluss der Installation alle Programme, die in der Zweigstelle benötigt werden, installiert und konfiguriert. Office-Lizenzen waren zum Teil vorhanden, eine geringe Zahl von 9 Stück musste noch nachgekauft werden. Benötigte Programme in der Zweigstelle in Dessau:

Office 2003 Basic (Word, Excel, Outlook)	Optionaler Browser Mozilla Firefox Version 2.0
Adobe Acrobat Reader 8.0	Irfan View
Free PDF	7Zip
Warenwirtschaftslösung	

Das Warenwirtschaftssystem der Zweigstelle musste nur installiert werden, da eine Fremdfirma die Konfiguration dieses Systems übernimmt. Da auch schon eine Webmail-Lösung in der Zweigstelle vorhanden war, die von einem Internet-Provider gehostet wird, musste auch kein Outlook eingerichtet werden. Die Lösung mit Microsoft Exchange als Messaging System wurde zwar im ersten Gespräch angesprochen, aber die Geschäftsführung wollte erst im nächsten Jahr wieder Geld in die EDV investieren. Als das Image erstellt war, wurde es von den Mitarbeitern der Zweigstelle noch einmal überprüft. Nach diesem Test habe ich das Betriebssystem mit Sysprep versiegelt und ein Image mittels Symantec Norton Ghost auf den Server kopiert. Die Verteilung des Images mithilfe eines Ghost Multicasts zeigte, dass das neue Netzwerk schnell und belastbar ist.

9.1 Konfiguration von WSUS an den Clients

In der Zweigniederlassung sind folgende Geräte vorhanden:

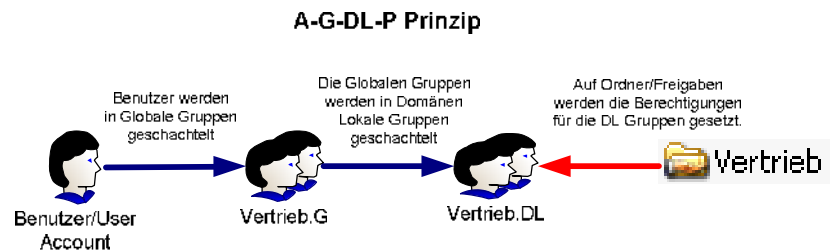
- 35 Windows XP Professional Client computers incl. Service Pack 2
- 3 Windows XP Professional Notebooks incl. Service Pack 2
- 2 Windows 2003 Server Standard R2 incl. Service Pack 2

In unserer Windows 2003 Server Umgebung mit einer Windows 2003 Domäne, die den Active Directory Dienst zur Verfügung stellt, werden Arbeiten an den Clients mittels Gruppenrichtlinien erheblich vereinfacht. Im Active Directory können Gruppenrichtlinien erstellt werden, die für die ganze Domäne oder einzelne Organisationseinheiten ange-

wandt werden. Da die Clients in der Zweigstelle in Notebooks Clients und Standard Clients unterteilt sind, muss ich die Gruppenrichtlinie auf beide Organisationseinheiten verknüpfen. Der Automatische Updateclient ist auf jedem Client/Server gestartet. Nun müssen die Updates nur noch vom Netzwerkadministrator freigegeben werden. Die Verteilung der Updates erfolgt dann nach dem konfigurierten Zeitschema.

9.2 Einrichten der Freigaben nach Kundenwunsch

In der Zweigstelle werden die Freigaben entsprechend der verschiedenen Abteilungen erstellt und zugeteilt. Jede Abteilung besitzt ein Abteilungslaufwerk, z.B. Vertrieb, auf diese Freigabe darf



nur der Vertrieb zugreifen. Für jeden Benutzer sollte allerdings auch ein privates Laufwerk angelegt werden, um rein benutzerbezogene Daten ablegen zu können. Ein drittes Laufwerk wird noch hinzugefügt, damit allgemeine Firmendaten zur Verfügung gestellt werden können. Die NTFS Berechtigungen werden nach dem AGDLP Prinzip vergeben. Um die gewünschten Ressourcen allen Benutzern richtig und schnell zuweisen können, erstelle ich ein Loginbatch, die den Benutzern über die Einstellungen im Active Directory Benutzer und Computer zugewiesen wird. Damit ich nur ein Script für die komplette Niederlassung schreiben muss, wird beim Login eines Benutzers überprüft, in welcher Abteilung er ist, durch diese Auswahlkriterien werden dann die entsprechenden Freigaben verbunden.

Abteilung	Freigegebener Ordner	Zugehörige Gruppe	Freigabe Berechtigung	NTFS Berechtigung
Verwaltung	Verwaltung	Verwaltung.DL	Authentifizierte Benutzer Vollzugriff	Lesen/-Schreiben/Ändern
Service	Service	Service.DL	Authentifizierte Benutzer Vollzugriff	Lesen/-Schreiben/Ändern
Vertrieb	Vertrieb	Vertrieb.DL	Authentifizierte Benutzer Vollzugriff	Lesen/-Schreiben/Ändern
Technik/-Lager	Technik	Technik.DL	Authentifizierte Benutzer Vollzugriff	Lesen/-Schreiben/Ändern
Alle	Allgemeine Firmendaten für alle	Alle.DL	Authentifizierte Benutzer Vollzugriff	Lesen/-Schreiben/Ändern
Jeder einzelne Benutzer	%username%	Benutzer	Administrator und der Benutzer Vollzugriff	Lesen/-Schreiben/Ändern

9.3 Einschränken der Benutzer mittels Gruppenrichtlinien

Gruppenrichtlinien dienen zur Arbeitserleichterung von Administratoren, mit Gruppenrichtlinien können bestimmte Rechte eingeschränkt, Software installiert oder Anmelde-/Abmeldescripts hinterlegt werden.

9.4 **Warum Gruppenrichtlinien?**

Der Vorteil der Gruppenrichtlinien ist, dass sie sehr differenziert für verschiedene Rechner und Benutzergruppen erstellt werden können. Wie vorhin schon beschrieben benötigt man für den WSUS Server auch Gruppenrichtlinieneinstellungen, mit dieser Richtlinie wird allen Clients im Netzwerk vorgegeben wo und in welchem Zeitabständen sie sich ihre Microsoft Updates vom WSUS-Server abholen müssen. Die Geschäftsführung und die EDV-Beauftragten in der Zweigstelle haben darauf bestanden, ihre Benutzer ebenfalls stärker einzuschränken. Deshalb habe ich eine weitere Gruppenrichtlinie erstellt, in der die Rechte der Benutzer der Niederlassung in Dessau eingeschränkt werden. Jetzt können keine Programme oder Tools von den Benutzern mehr installiert werden, des Weiteren können keine Änderungen in der Systemsteuerung, Netzwerkumgebung und Registry vorgenommen werden. Gruppenrichtlinien können auf zwei verschiedene Arten konfiguriert werden, zum einen nur computerbezogen um die Clientcomputer im Voraus schon einzuschränken und zum anderen benutzerbezogen. Gruppenrichtlinien werden mit OUs verknüpft, deshalb werden in der Hardware OU in der Zweigstelle nur Gruppenrichtlinien hinterlegt, die sich auf die Computerkonfiguration beziehen. Für Administratoren sind Gruppenrichtlinien in gewachsenen Netzwerkumgebungen kaum noch wegzudenken und ein wichtiges Werkzeug um schnell und effizient etwas umzustellen oder hinzufügen zu können. Im Augenblick werden Gruppenrichtlinien nur für die Rechtebeschränkung erstellt, nicht für die automatische Softwareverteilung. Seit Windows 2003 Server gibt es ein weiteres wichtiges Tool zur Verwaltung von Gruppenrichtlinien die Gruppenrichtlinienmanagement Konsole. Die Anmeldescripts in der Zweigniederlassung wurden ebenfalls mittels einer Gruppenrichtlinie hinterlegt.

9.5 **Wo werden Gruppenrichtlinien eingesetzt?**

GPO auf Clients

- Über Gruppenrichtlinien können Einstellungen für Outlook und das System selbst eingestellt werden. Auch Funktionen wie Windows Update, die Verfügbarkeit von Diensten und Berechtigungen auf Dateien und Registrierungsschlüssel sind einstellbar.

GPO auf User

- Benutzerkonten können über GPOs im Bezug auf den Explorer und andere Programme konfiguriert werden
- Generell gilt aber auch hier, dass ohne Planung das Ganze schnell in Chaos ausartet.

GPO auf Server

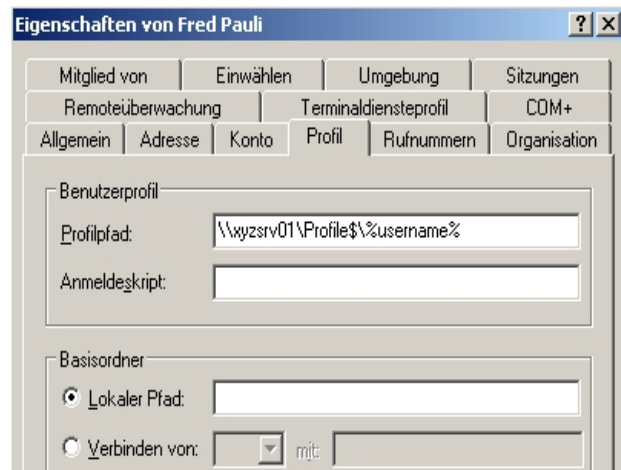
- Auch auf Servern sind GPOs hilfreich, um z.B.: die Größe des Eventlog, Windows Update oder SNMP Einstellungen zu konfigurieren.

In der Zweigstelle ist in der Domäne eine Gruppenrichtlinie für Hardware (Computerkonfiguration) / Clients und für die Benutzer (Benutzerkonfiguration) vorhanden.

9.6 Erstellen der Benutzerprofile

Dadurch dass auch mal mehrere Benutzer in der Zweigstelle an einem PC arbeiten, stellt sich die Frage, wo die persönlichen Einstellungen gespeichert sind. Dieses Problem löse ich durch „Servergespeicherte Profile“. Diese Profile enthalten von jedem Benutzer folgende Einstellungen:

- Bildschirmhintergrund
- Bildschirmschoner
- Größe und Positionen von Icons
- Internetoptionen (Favoriten)
- Umleitung von „Eigene Dateien“
- Eigenschaften der Taskleiste



Persönliche Programmgruppen im Startmenü werden individuell eingestellt. Diese Dinge soll der jeweils andere Benutzer nicht verändern, damit man beim nächsten Mal alles wieder findet. Damit die servergespeicherten Profile leichter erstellt werden, muss im Active Directory bei den Benutzern ein Profilpfad eingegeben werden. Damit ich diesen Vorgang auch automatisieren konnte, habe ich mit einer Variable gearbeitet (%username%). Diese Variable erstellt dann von selbst einen Ordner im Profile-Stammverzeichnis mit dem jeweiligen Benutzernamen.

Dateiberechtigungen am Profil-Stammverzeichnis:

Name	Berechtigung	Typ	Übernehmen für
Administratoren	Vollzugriff	Zulassen	Für diesen und untergeordnete Ordner
System	Vollzugriff	Zulassen	Für diesen und untergeordnete Ordner
Ersteller/Besitzer	Vollzugriff	Zulassen	Für diesen und untergeordnete Ordner

9.7 Bereitgestellte Ressourcen per Script bereitstellen

Um nicht jedem Clientcomputer manuell die benötigten Netzlaufwerke und Drucker einrichten zu müssen, wird dieser Vorgang mithilfe eines Anmeldescripts automatisiert. Anmeldescripts haben den Vorteil, dass sie nur einmal erstellt werden müssen bzw. bei Änderungen oder Neuerungen im Netzwerk, z.B. neue Drucker und Freigaben nur im Script abgeändert oder hinzugefügt werden müssen. Die Anmeldescripts wurden in zwei verschiedene Gruppen unterteilt und außerdem wurde noch ein Abmeldescript erstellt. Ein Script verbindet die Netzlaufwerke und loggt Anmeldungen mit, das andere verbindet nur die Drucker. Mit diesem Trick wird vermieden, dass größere Probleme bei der Anmeldung auftreten. Wenn z.B. die Drucker nicht verbunden werden können, kann man davon ausgehen, dass mit dem Druckerscript etwas nicht stimmt. Mithilfe des Anmeldescripts in der Zweigstelle wird hier auch noch mitgeloggt, wer sich „wo“ und „wann“ an- und abmeldet. Scripte erleichtern den administrativen Aufwand im Netzwerk.

Wenn alles gut geplant und richtig umgesetzt worden ist, sind auch die Benutzer zufrieden. (Anhang [D] Loginscripts)

10 Sicherungstechnische Maßnahmen

In der Nebenstelle war bereits eine 3000VA USV der Firma APC vorhanden. Diese wurde dann über einen seriellen Port an Server 1 angeschlossen. Nach Installation und Konfiguration der PowerChute Software, wird der Server 1 heruntergefahren sobald der Strom länger als 10 Minuten ausfällt. Diese Software veranlasst außerdem nach 6 Minuten das Starten einer Batchdatei, die den Server 2 ordnungsgemäß herunterfährt.

Die Leitung in Dessau wollte im Augenblick keine weiteren Investitionen in die EDV machen, deshalb verzichtete sie darauf einen Streamer für die täglichen und wöchentlichen Backups anzuschaffen. Ich habe den Geschäftsführer und den EDV-Beauftragten auf die Bedeutung regelmäßiger Backups hingewiesen und ihnen klar gemacht, dass ein Raid-System kein Ersatz für eine Backuplösung ist. Trotzdem wollen sie diese Investition erst im nächsten Jahr tätigen. Zur Sicherheit habe ich trotzdem ein vollständiges Backup des Servers 1 auf eine externe SCSI-Platte unserer Firma gemacht, dies anschließend dem Kunden erklärt und mit ihm vereinbart, dass wir dieses Grundsystem als offline Sicherung bei uns in der Firma aufbewahren. Dafür habe ich eine schriftliche Einverständniserklärung des Kunden erhalten.

11 Test des EDV-Systems

Zum Abschluss folgt ein ausführlicher Funktionstest aller Komponenten und Funktionalitäten. Da die Clients mit dem Server kommunizieren und alle gewünschten Funktionen gegeben sind, beschränke ich mich auf die Server, die vorhandene USV Anlage und die redundant ausgelegte Serverhard- und Software. Um sicherzustellen, dass alle Redundanzen gegeben sind, teste ich zum Schluss das neue System. Als erstes fahre ich Server eins herunter und probiere, ob ich mich mit einem Client noch anmelden kann, ob der Client eine IP-Adresse bekommt und ob das Domainnamesystem noch funktioniert. Diese Funktionen waren gegeben, aber den Usern standen natürlich keine Netzwerklaufwerke oder ihre Userprofile zur Verfügung. Als zweiten Test fahre ich Server zwei herunter und teste diese Funktionen noch einmal. Dieses Mal waren alle Funktionen voll gegeben, bis auf die Drucker, denn diese Freigaben befinden sich auf Server 2 und wenn dieser down ist, kann nichts mehr gedruckt werden. Da in beiden Servern redundante Netzteile verbaut worden sind, werden diese zum Schluss auch noch einem kleinen Test unterzogen. Das abwechselnde Entfernen einer Stromverbindung führte auch zu keinen Einschränkungen. Nachdem ich die USV vom Stromnetz trennte, erhielt ich sowohl eine akustische Benachrichtigung als auch eine Benachrichtigung am Monitor. Die Funktionen des Shutdownscripts wurden auch noch getestet und beide Server haben sich ordnungsgemäß heruntergefahren. Um die Raidcontroller sowie die Hotplug Fähigkeit der Festplatten zu testen, wird zur Fehlersimulation noch eine Festplatte herausgezogen um sicherzustellen, dass bei einem Festplattenschaden weitergearbeitet werden kann. Dieser Test verlief auch problemlos.

12 Übergabe und Einführung der Mitarbeiter in das neue System

Vor der Übergabe des neuen Systems wurden nochmals alle von mir durchgeführten Arbeiten ausführlich besprochen. Mit Hilfe der neuen Dokumentation können sich neue Administratoren oder EDV-Beauftragte einfacher in das System einarbeiten. Zu guter Letzt werden die Mitarbeiter der Firma XYZ in das neue EDV-System eingewiesen. Da die Mitarbeiter schon alle relativ gute Kenntnisse in Windows XP hatten, fällt es mir sehr leicht, ihnen die neuen Features zu präsentieren. Am besten haben sich die Mitarbeiter über die dynamischen Userprofile gefreut, da solch ein Feature in der alten Umgebung ebenfalls gefehlt hat.

13 Fazit / Ausblick

Projektschritte	Geplanter Aufwand	Tatsächlicher Aufwand
Durchführung einer Ist-Analyse	1	1,5
Erarbeitung eines Soll-Konzepts	3	1,5
Installation der Server	5	5
Konfiguration der Server	8	8
Erstellen und verteilen der Clientimages	4	6
Installation / Konfiguration von WSUS	2	1,5
Erstellen der Anmeldedescripts per Batch	1	1,5
Erstellen der Leistungs- Auditing Monitore	3	1
Erstellen der Benutzer und Freigaben	5	5
Schulung der Benutzer	3	5
Gesamtaufwand	35	36

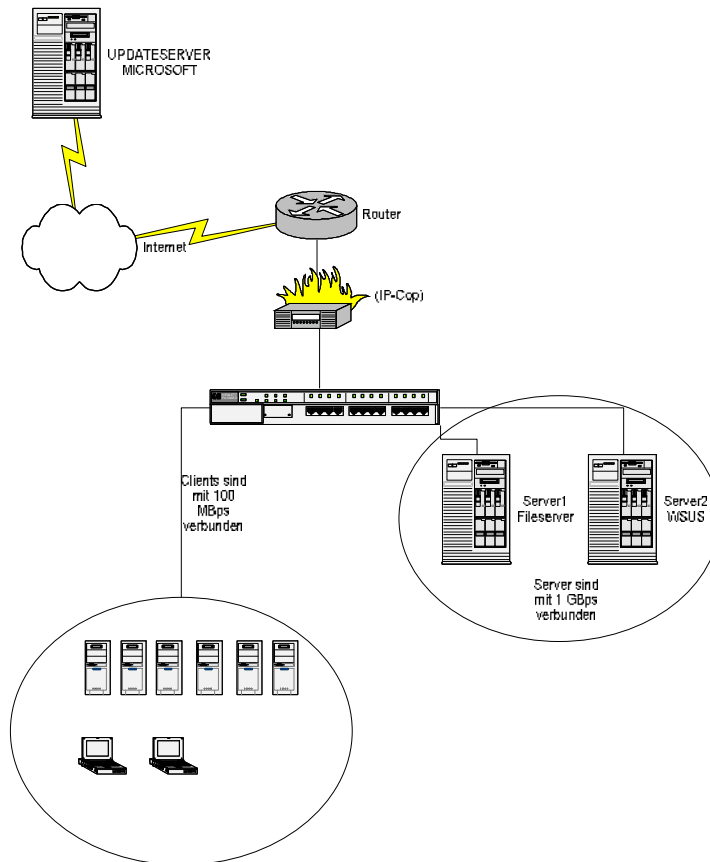
Durch die gute Vorplanung und Zusammenarbeit mit der Firma XYZ konnten sämtliche Vorgaben eingehalten werden. Alle geplanten Arbeitsgänge wurden weitgehend fehlerfrei durchlaufen. Die Datenübernahme vom alten Linux-System auf das neue Windows-System verlief problemlos. Durch den Einsatz von bereits vorhandener, jedoch geeigneter Hardware konnten erfreulicherweise die entstandenen Kosten relativ gering gehalten werden. Die einzige größere Investition waren letztendlich die zwei Windows 2003 Serverlizenzen und die entsprechenden Workstation CALs. Die Entscheidung der Firma XYZ auf ein neues System umzustellen halte ich für vollkommen richtig, da die Open Source Lösung mit Linux auf Dauer teurerer geworden wäre als die jetzige Lösung mit den beiden Windows 2003 Servern. (Grund: Nach dem Ankauf der Niederlassung in Dessau und der Angleichung der Netzstruktur in Dessau an das Netz der Zentrale können nun in beiden Geschäftsstellen dieselben Softwareapplikationen verwendet werden. Außerdem kann ein Großteil der administrativen Aufgaben in Zukunft von der Hauptstelle aus übernommen werden.)

Meiner Meinung nach hat die Firma XYZ mit dieser Windows Server 2003 Lösung auch die besten Möglichkeiten ihr System weiter aufzubauen. In der Netzwerkinfrastruktur herrscht wieder Ordnung, was früher leider nicht der Fall war. Die Ausfallsicherheit wurde durch das neue System deutlich erhöht. Abschließend kann ich feststellen, dass das Projekt zur Zufriedenheit aller Beteiligten durchgeführt wurde. Und die Netzwerkperformance wurde deutlich gesteigert.

Anhänge:

ANHANG A1

Die neue Netzwerkinfrastruktur der Firma XYZ



ANHANG A2

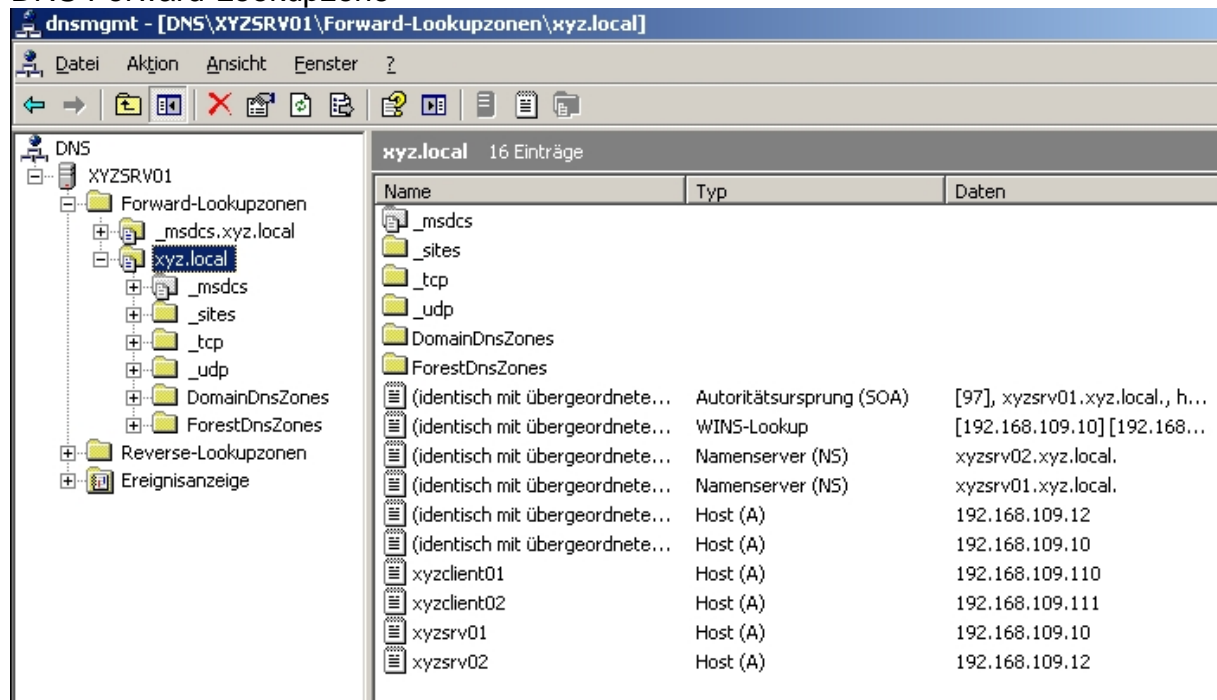
Domänenstruktur der Zweigniederlassung in Dessau

name	typ	beschreibung
Firmenadmin XYZ	Benutzer	
Tobias Pongratz	Benutzer	

- xyz.local
 - _GPO-Vorlagen
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Users
 - xyz.Admins
 - xyz.Dessau
 - HARDWARE
 - Clients
 - Notebooks
 - Server
 - Sonstiges
 - USER
 - Service
 - Technik
 - Lager
 - Reparatur
 - Vertrieb
 - IT
 - Mobilfunk
 - Unterhaltungsele
 - xyz.Schoenberg
 - xyz.Verwaltung
 - BuHa
 - FIBu
 - LoBu
 - Geschäftsführung
 - Management
 - Prokura

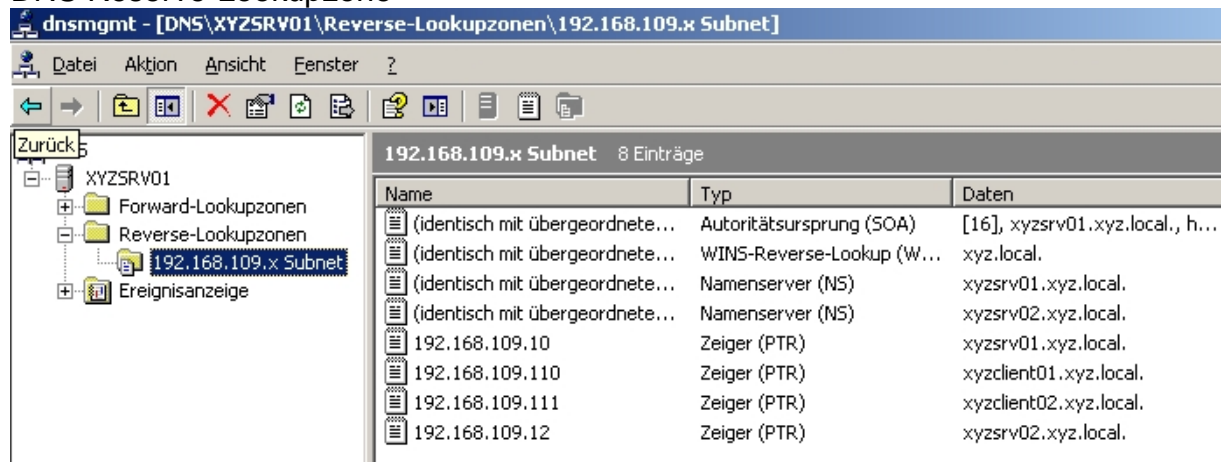
ANHANG B

DNS Forward-Lookupzone



Name	Typ	Daten
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(identisch mit übergeordnete...)	Autoritätsursprung (SOA)	[97], xyzsrv01.xyz.local., h...
(identisch mit übergeordnete...)	WINS-Lookup	[192.168.109.10][192.168...
(identisch mit übergeordnete...)	Namensserver (NS)	xyzsrv02.xyz.local.
(identisch mit übergeordnete...)	Namensserver (NS)	xyzsrv01.xyz.local.
(identisch mit übergeordnete...)	Host (A)	192.168.109.12
(identisch mit übergeordnete...)	Host (A)	192.168.109.10
xyzclient01	Host (A)	192.168.109.110
xyzclient02	Host (A)	192.168.109.111
xyzsrv01	Host (A)	192.168.109.10
xyzsrv02	Host (A)	192.168.109.12

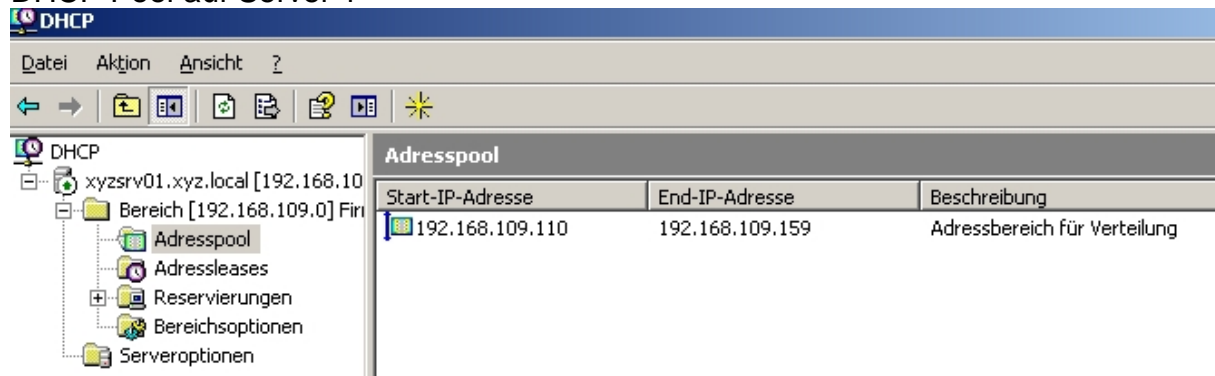
DNS Reverse-Lookupzone



Name	Typ	Daten
(identisch mit übergeordnete...)	Autoritätsursprung (SOA)	[16], xyzsrv01.xyz.local., h...
(identisch mit übergeordnete...)	WINS-Reverse-Lookup (W...)	xyz.local.
(identisch mit übergeordnete...)	Namensserver (NS)	xyzsrv01.xyz.local.
(identisch mit übergeordnete...)	Namensserver (NS)	xyzsrv02.xyz.local.
192.168.109.10	Zeiger (PTR)	xyzsrv01.xyz.local.
192.168.109.110	Zeiger (PTR)	xyzclient01.xyz.local.
192.168.109.111	Zeiger (PTR)	xyzclient02.xyz.local.
192.168.109.12	Zeiger (PTR)	xyzsrv02.xyz.local.

ANHANG C

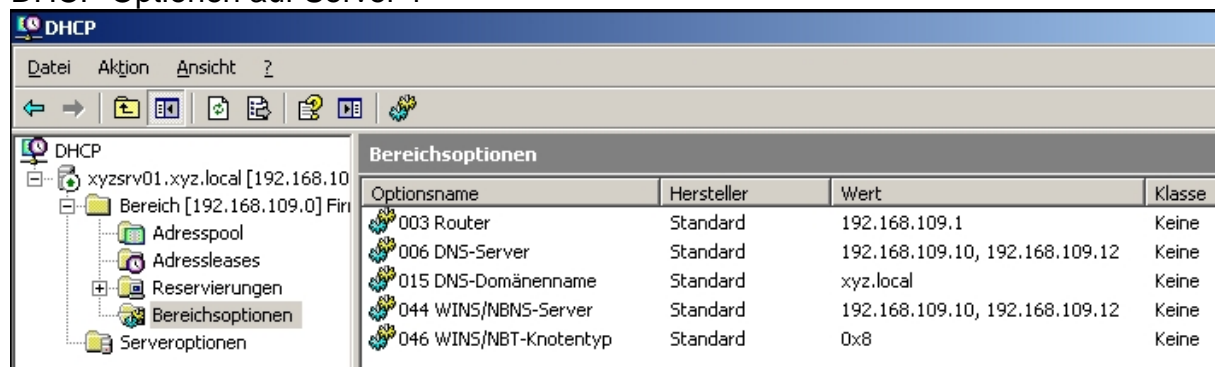
DHCP Pool auf Server 1



The screenshot shows the DHCP console for a server named 'xyzsrv01.xyz.local [192.168.10.10]'. The left pane shows a tree view with 'Bereich [192.168.109.0] Firma' expanded to show 'Adresspool'. The right pane displays a table for the selected address pool.

Start-IP-Adresse	End-IP-Adresse	Beschreibung
192.168.109.110	192.168.109.159	Adressbereich für Verteilung

DHCP Optionen auf Server 1



The screenshot shows the DHCP console for the same server. The left pane shows 'Bereichsoptionen' selected under the scope. The right pane displays a table of configured options.

Optionsname	Hersteller	Wert	Klasse
003 Router	Standard	192.168.109.1	Keine
006 DNS-Server	Standard	192.168.109.10, 192.168.109.12	Keine
015 DNS-Domänenname	Standard	xyz.local	Keine
044 WINS/NBNS-Server	Standard	192.168.109.10, 192.168.109.12	Keine
046 WINS/NBT-Knotentyp	Standard	0x8	Keine

Der WINS Server



The screenshot shows the WINS console for a server named 'XYZSRV01 [192.168.109.10]'. The left pane shows 'Aktive Registrierungen' selected. The right pane displays a text box with instructions on how to manage the active registrations.

Aktive Registrierungen

An dieser Stelle können Sie die Computer- und Gruppeneinträge der WINS-Datenbank aufführen. Klicken Sie auf "Aktion" und dann auf "Einträge anzeigen", um die Einträge anzuzeigen. Im Dialogfeld "Einträge anzeigen" können Sie die Einträge folgendermaßen filtern:

- * Klicken Sie auf die Registerkarte "Eintragszuordnung", um nach NetBIOS-Namen oder IP-Adresse zu filtern. Sie können auch nach Subnetzmaske filtern, wenn Sie nach IP-Adresse filtern.
- * Klicken Sie auf die Registerkarte "Eintragsbesitzer", um nach Besitzer zu filtern.
- * Klicken Sie auf der Registerkarte "Eintragstypen", um nach Eintragstyp zu filtern. Sie können auch neue Eintragstypen hinzufügen, bestehende Eintragstypen bearbeiten oder von Ihnen hinzugefügte Eintragstypen löschen.

ANHANG D

Shutdownscript für die USV Software

```
@echo off  
shutdown -m \\192.168.109.12 -s -t 05 -f
```

Loginscript für die Netzlaufwerke

@echo off

REM Protokollierung An und Abmeldung

```
echo %username%;%computername% >> \\xyzsrv01\Protokoll$\Anmeldung.txt
date /T >> \\xyzsrv01\Protokoll$\Anmeldung.txt
time /T >> \\xyzsrv01\Protokoll$\Anmeldung.txt
echo -----
>>\\xyzsrv01\Protokoll$\Anmeldung.txt
```

REM Netzlaufwerke löschen

```
net use I: /delete
net use P: /delete
net use Y: /delete
net use Z: /delete
```

REM Standard Netzlaufwerke verbinden

```
net use I: %logonserver%\NETLOGON
net use P: \\xyzsrv01\Users$\%username%
net use Z: \\xyzsrv01\XYZShare$
```

REM für jede ABTEILUNG das Netzlaufwerk verbinden

```
I:\anmeldung\ifmember.exe Service.G
if not errorlevel 1 goto weiter1
net use Y: \\xyzsrv01\Service$
```

```
:weiter1
I:\anmeldung\ifmember.exe Vertrieb.G
if not errorlevel 1 goto weiter2
net use Y: \\xyzsrv01\Vertrieb$
```

```
:weiter2
I:\anmeldung\ifmember.exe Verwaltung.G
if not errorlevel 1 goto weiter3
net use Y: \\xyzsrv01\Verwaltung$
```

```
:weiter3
I:\anmeldung\ifmember.exe Technik.G
if not errorlevel 1 goto ENDE
net use Y: \\xyzsrv01\Technik$
:ENDE
net use I: /delete
exit
```

Loginscript für die Netzwerkdrucker

```
@echo off

REM für jede ABTEILUNG den Drucker verbinden

net use I: %logonserver%\NETLOGON

I:\con2prt.exe /f

I:\anmeldung\ifmember.exe Service.G
if not errorlevel 1 goto weiter1

I:\con2prt.exe /cd \\xyzsrv02\HPLaserTECHNIK
I:\con2prt.exe /cd \\xyzsrv02\HPLaserSERVICE

:weiter1
I:\anmeldung\ifmember.exe Vertrieb.G
if not errorlevel 1 goto weiter2

I:\con2prt.exe /cd \\xyzsrv02\HPLaserSERVICE
I:\con2prt.exe /cd \\xyzsrv02\HPLaserTechnik
I:\con2prt.exe /cd \\xyzsrv02\HPLaserVERTRIEB

:weiter2
I:\anmeldung\ifmember.exe Verwaltung.G
if not errorlevel 1 goto weiter3
I:\con2prt.exe /cd \\xyzsrv02\HPLaserLoBu
I:\con2prt.exe /cd \\xyzsrv02\HPLaserFiBu
I:\con2prt.exe /cd \\xyzsrv02\HPLaserProkura
I:\con2prt.exe /cd \\xyzsrv02\HPLaserManagement
I:\con2prt.exe /cd \\xyzsrv02\HPLaserVerwaltung

:weiter3
I:\anmeldung\ifmember.exe Technik.G
if not errorlevel 1 goto ENDE

I:\con2prt.exe /cd \\xyzsrv02\HPLaserSERVICE
I:\con2prt.exe /cd \\xyzsrv02\HPLaserTECHNIK

:ENDE
net use I: /delete
end
```

Glossar, Begriffserklärung

OU - Organisationseinheit

Mithilfe von Organisationseinheiten können Abteilungen/Unternehmensbereiche geteilt werden und auf die verschiedenen OUs können unterschiedliche Rechte oder Gruppenrichtlinien gelegt werden, in OUs sind meistens Benutzer oder Computer hinterlegt.

Gruppenrichtlinie (Group Policies) GPO:

Ist eine Regel, die z.B. wie in meinem Projekt festlegt, dass sich alle Clientcomputer ihre Windowsupdates vom WSUS Server ziehen.

Domäne

In einem Netzwerk mit Domain Controller können mehrere Clientcomputer zu einer Domäne zusammengefasst werden. Im Unterschied zu den Arbeitsgruppen von Windows 9x/ME kann zentral am Domain Controller festgelegt werden, welche Benutzer sich mit welchem Passwort anmelden dürfen, und auf welche Ressourcen der Benutzer Zugriff hat. In einer Domäne können mehrere Domaincontroller vorhanden sein um das Netzwerk ausfallsicher zu gestalten.

Active Directory (AD)

Ist ein skalierbarer, hierarchischer Verzeichnisdienst zur zentralen Verwaltung aller für das Netzwerk relevanter Ressourcen.

DNS Domain Name System

- DNS ist eine hierarchische verteilte Datenbank, die Zuordnungen von Computernamen in IP und von IP in Computernamen enthält

WINS – Windows Internet Name Service

- WINS löst Netbios Namen auf.
- Erleichtert älteren Clients die Namensauflösung

DHCP – Dynamic Host Configuration-Protocoll

- DHCP stellt einen IP-Standard dar, der zur Verwaltung und automatischen Vergabe von Client IP-Adressen verwendet wird.

Image:

Abbild einer Festplatte oder Partition

Im Unterschied zu einer Kopie oder einem Backup enthält ein Image Informationen über die Struktur des Originalspeichers. Dies ermöglicht es, schnell exakte Kopien eines Datenträgers zu erstellen.

IP-Adresse:

Ist eine eindeutig im Netzwerk vergebene Adresse die entweder manuell oder automatisch per DHCP vergeben wird.

Patch/Hotfix:

Ist ein Sicherheitsupdate, das diverse Sicherheitslücken behebt. Patch Day bei Microsoft ist jeden zweiten Dienstag im Monat. (http://de.wikipedia.org/wiki/Patch_Day)

Raid 1:

Raidsystem, das mit 2 physikalischen Platten erstellt wurde, um sich vor einem Festplattencrash zu schützen.

WSUS:

Windows Server Update Service, der von Microsoft kostenlos zur Verfügung gestellt wird, um die Computer im Netzwerk updaten zu können. Mit WSUS werden die Sicherheitsupdates auch nur einmal vom Internet heruntergeladen.

Quellenangaben:

<http://www.microsoft.com/germany/technet/datenbank/articles/600849.msp>

<http://www.wsus.de/>

<http://www.microsoft.com/germany/windowsserver2003/technologien/updateservices/default.msp>

WSUS StepbyStep.doc von Microsoft (MS Whitepaper)

<http://support.microsoft.com/kb/322692/de>

<http://www.microsoft.com/technet/scriptcenter/default.msp>

Bücher:

- Microsoft Official Course 2163A Warten einer Windows Server 2003 Umgebung
- Microsoft Official Course 2183A Implementieren, Verwalten und Warten einer Windows Server 2003 Netzwerkinfrastruktur: Netzwerkdienste
- Microsoft Official Course 2145A Verwalten einer Windows Server 2003 Umgebung

Erklärung zur betrieblichen Projektarbeit

Erklärung des Prüfungsteilnehmers

Ich versichere durch meine Unterschrift, dass ich das Projekt und die dazugehörige Dokumentation selbständig und ohne fremde Hilfe angefertigt und alle Stellen, die ich wörtlich oder annähernd wörtlich aus Veröffentlichungen entnommen habe, als solche kenntlich gemacht habe. Die Arbeit hat in dieser Form keiner der anderen Prüfungssituationen vorgelegen.

Ort, Datum

Unterschrift des Prüfungsteilnehmers

Erklärung des Ausbildungsbetriebes

Wir versichern, dass das Projekt wie in der Dokumentation dargestellt, in unserem Unternehmen durchgeführt worden ist.

Ort, Datum

Unterschrift des Ausbildungsbetriebs