

Windows IT Pro

Das Magazin für den Windows-Administrator

Messaging & Groupware

Praxistest: Exchange-Alternative
Sicherheit: E-Mail-Authentifizierung
Entlastung: Archivierung der Mail

LAB-REPORT

- Software für das Training
- Flexible Festplatte
- Test: Automatischer Datenabgleich

SPECIAL

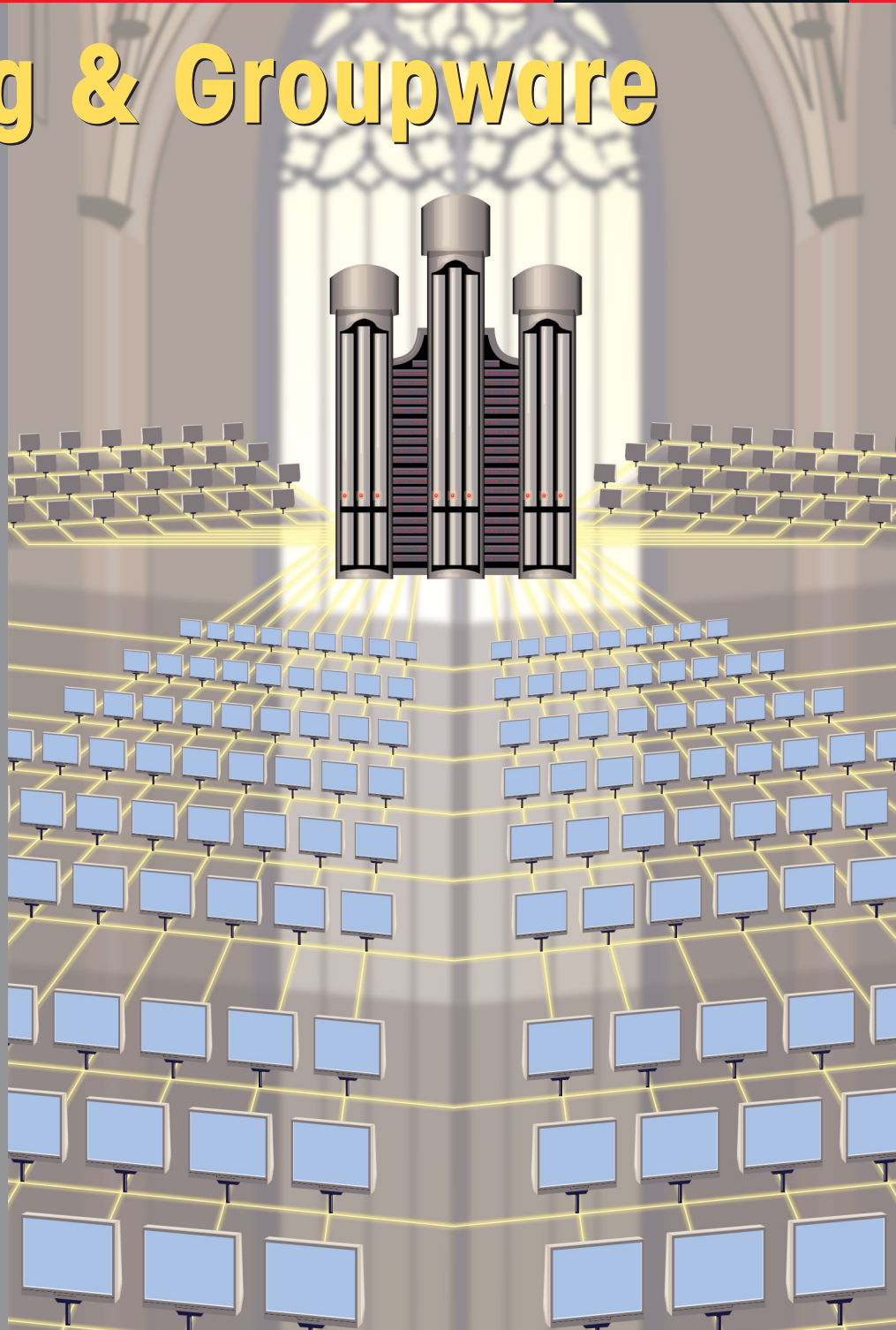
- EFS und Online-Dateien
- Exchange Server SP2

TOOLKIT

- Virenschutz vollautomatisch im Netz
- Skripting-Lösungen: Ordnung ins Verzeichnis bringen und fehlerlose Skripts schreiben

Marktübersicht:

Remote-Access-Lösungen



**Sonderdruck
für Schmidt's LOGIN**

Keep IT simple

von Roland Lötzerich

Geht es nach Microsoft, so gibt es wohl kaum noch Netzwerke, die mit dem „alten“ Server-System Windows NT 4 arbeiten. Aber natürlich wissen alle Fachleute, dass noch viele NT-4-Installation ihrer Migration harren. Hier erläutert ein Experte, welche Klippen bei solch einer Migration auftreten können und wie man sie umschiffen kann.

Ohne Zweifel stellt die Migration eines kompletten Unternehmensnetzwerkes auf Windows 2003 ist eine große Herausforderung dar. Das gilt insbesondere dann, wenn mehrerer Niederlassungen vorhanden sind, von denen sich einige vielleicht sogar im Ausland befinden: In diesen Fällen kann der Aufwand für die Koordinierung und Abstimmung den Aufwand für die eigentliche Umstellung sogar deutlich übersteigen. Ob ein Single- oder ein Multi-Domain-Modell geeignet ist, wie Domains und Organisational Units (OUs) strukturiert werden und wer das Ganze schließlich wie verwalten soll – all das sind Fragen, die schon im Vorfeld geklärt werden müssen.

Trotz solcher Vorbehalte ist eine Migration durchaus nach dem Leitsatz „Keep IT simple“ und mit relativ geringem Aufwand zu realisieren. Dazu braucht man vor allem Erfahrung und Geduld. Zunächst sollte ein solches Projekt in verschiedene Phasen eingeteilt werden:

- Vorbereitung und Planung,
- Design der Active Directory-Struktur,

- Implementierung des Active Directory und
- Umstellung der Workstations.

In der ersten Phase, der Vorbereitung und Planung, sollten die durchzuführenden Arbeiten bereits vor Projektbeginn grob erfasst und abgeschätzt werden. Diese Informationen bilden dann die Grundlage für die Erstellung der Unterlagen zur Projektgenehmigung durch das Management. Danach folgen die Abschätzung der Kosten sowie die Erstellung des Projektplanes und der -dokumentation. Nach der Genehmigung des Projektes wird die erste Phase mit der Schulung der Projektmitarbeiter abgeschlossen.

Stehen beispielsweise nicht alle Informationen bezüglich Hardware- und Softwarekompatibilität oder der Strategien zur Adressvergabe oder Absicherung zur Verfügung, so empfehlen sich bestimmte Vorstudien. Zudem muss die Frage des angemessenen Migrationsweges geklärt werden: Soll eine direkte Migration (In-Place Upgrade) der vorhandenen Installation durch-

geführt werden? Oder doch eine Neuinstallation von Windows 2003 (Restrukturierung)? Außerdem besteht noch die Möglichkeit, zunächst ein In-Place-Upgrade durchzuführen und erst danach zu restrukturieren. Dieses Vorgehen wird am Ende des Artikel noch genauer erläutert.

Wenn diese Entscheidungen gefallen sind, sollte ein Grobkonzept entwickelt werden. Eine Voraussetzung dafür ist es, dass alle notwendigen Informationen vorliegen – auch die aus den Niederlassungen, die auf Grund anderer lokaler Marktgegebenheiten andere Anforderungen an die Infrastruktur stellen können. Der Aufwand für Vorstudien und Dokumentation variiert. So verlangt das Management oft im Rahmen der Projektgenehmigung noch Entscheidungstabellen für größere Investitionen. Hier geht es zum Beispiel darum, welche Windows-Version eingesetzt werden soll oder ob Linux die günstigere Alternative wäre. Oder es geht um das Office Paket (2003, XP oder StarOffice) sowie um die Auswahl des Installations- und des Asset Management-Tools.

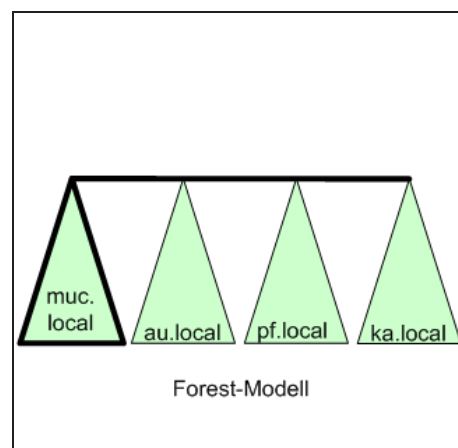
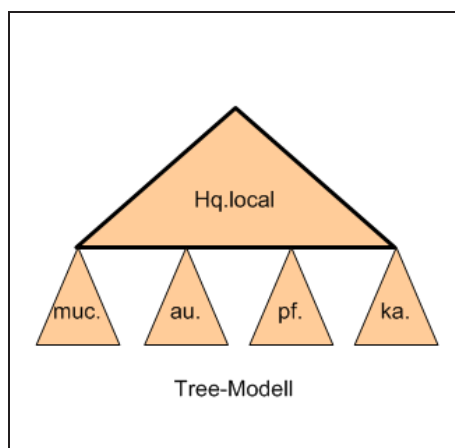
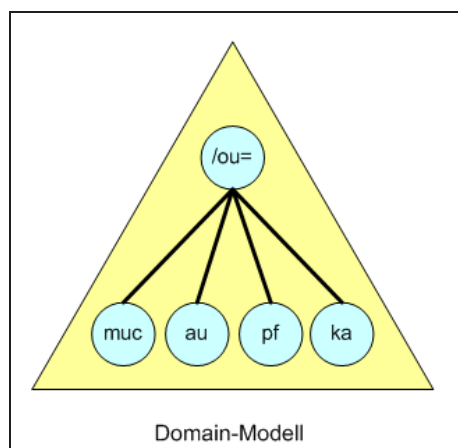


Bild 1. Das Design der Active-Directory-Struktur: Da der Ansatz mit mehreren Forests in der Regel vermieden werden sollte, stehen dann entweder das Domain-, das Tree- oder das Forest-Modell zur Auswahl (Quelle: Schmidt's Login).

Glossar: Wichtige Komponenten des Active Directory

AD-Domains:

AD Domains sind durch einen DNS-Namen beschrieben und besitzen, wie NT-Domains, einen NetBIOS-Namen. Alle Domains in einem Forest (siehe unten) haben folgendes gemeinsam:
Schema: formale Definition aller Objekte, deren Eigenschaften und Beziehungen;
Global Catalog (GC): teilweise Replikation aller Objekte im Forest;
Konfiguration: unternehmensweite Konfigurations-Informationen inklusive der Standorte und Netzwerk-Dienste (zum Beispiel Exchange)

Forests und Trees:

Ein Tree ist eine hierarchische Anordnung von Domains in einem fortlaufenden Namensraum (beispielsweise „HQ.LOCAL“ als Stamm-Domain und „RES.HQ.LOCAL“ als untergeordnete Domain). Alle Domains in einem Tree haben einen zweiseitigen transitiven Trust zwischen über- und untergeordneter Domain.

Ein Forest stellt dann eine Gruppierung von Domain Trees in einem fortlaufenden oder in einem unabhängigen Namensraum dar. Dabei ist die erste Domain in einem Forest die so genannte Forest-Wurzel, die weder umbenannt noch entfernt werden kann. Der Name des Forest ist gleich dem ersten Tree im Forest. Im Forest existieren zweiseitige transitive Trusts zwischen allen Stamm-Domains aller Trees.

Man sollte vermeiden, mehr als einen Forest in einem Unternehmen zu implementieren. Insbesondere wenn vorgesehen ist, Exchange 2000/2003 einzusetzen, da eine „Exchange 2000 Organisation“ identisch mit einem Forest ist. Es ist nicht möglich, diese auf mehrere Forests auszuweiten.

Organisational Unit (OU):

OUs bilden eine nützliche Art von Verzeichnisobjekten in den Domains. Sie sind Active Directory-Container, in denen Benutzer, Gruppen, Computer und wiederum andere OUs organisiert werden können. Dabei können dann auch Objekte aus anderen Domains in einer OU enthalten sein. Eine OU stellt die kleinste Einheit dar, der Gruppenrichtlinieneinstellungen (GPOs) zugewiesen oder an die Administratorrechte delegiert werden können. Mit Hilfe von OUs lassen sich innerhalb einer Domain spezielle Container erstellen, die die administrativen Strukturen innerhalb der Organisation widerspiegeln.

Obwohl diese OUs gute Möglichkeiten bieten, um eine Domain zu strukturieren, ist es nicht ratsam, die gesamte Organisation 1:1 in solchen „administrativen Einheiten“ abzubilden. Oft ist die Versuchung groß, jeder Abteilung an jedem Standort eine OU zuzuweisen. Da aber jede OU separat verwaltet werden muss, endet das in aller Regel in einem administrativen Alptraum. OU-Strukturen sollten daher ausschließlich am Nutzen ausgerichtet und selbsterklärend sein. Vor dem Anlegen einer OU muss geklärt werden, wofür sie verwendet und von wem sie administriert werden soll.

Top-Level OUs sollten innerhalb eines Unternehmens (=Forest) standardisiert werden. Da die LOGON-Zeit mit der Anzahl und Schachtelungstiefe der OUs steigt, sollte ihre Schachtelungstiefe 10 nicht übersteigen. Die Delegation von administrativen Rechten sollte stets auf der OU-Ebene und nicht auf der Objekt-Ebene stattfinden.

Der nächste Schritt befasst sich mit dem DNS-Design: In Unternehmen, die bereits über eine DNS-Infrastruktur verfügen, empfiehlt sich der Aufbau einer zusätzlichen DNS-Infrastruktur für Windows 2003 auf allen AD-Domain-Controllern. Dafür muss zunächst der zu verwendende Namensbereich für die AD-Struktur festgelegt werden. Dieser Name muss nicht im Internet (IANA) registriert sein, da er lediglich im Intranet verwendet wird. Außerdem sollte dieser Name möglichst „neutral“ gewählt werden. Das bedeutet, dass er nicht gleich dem Firmennamen sein sollte, denn ein Umbenennen der AD-Struktur ist nur mit großem Aufwand und auch nur möglich, wenn Exchange 2000/2003 nicht zum Einsatz kommt.

Bei der IETF existiert ein Draft, (<http://www.ietf.org/proceedings/99nov/I-D/draft-ietf-dnsind-local-names-07.txt>), in dem zur Verwendung im Intranet die Top-Level Domain „.local“ vorgeschlagen wird, speziell wenn der lokale Adressbereich nach RFC1918 zum Einsatz kommt. Ein geeigneter, neutraler Name wäre dann beispielsweise „HQ.LOCAL“.

An dieser ist allerdings ein Hinweis wichtig: Das Multicast-DNS von Apple verwendet die Domain „.local“ im eigenen Rendezvous-Protokoll. Diese Vorgehensweise ist für einfache Umgebungen gedacht, in denen keine DNS-Infrastruktur zur Verfügung steht. Grundsätzlich stellt die Existenz einer Domain „.local“ in diesem Zusammenhang kein Problem dar, weil MAC OS so konfigu-

riert werden kann, dass es „.local“-Namen per Unicast auflöst. Alle anderen Geräte sind nicht betroffen, weil für DNS und Apples Multicast-DNS verschiedene Ports verwendet werden.

Daran anschließend geht es an die Abschätzung der Projektkosten: Anhand eines groben Projektplans lassen sich die Kosten vorab schätzen. Ist dies nicht möglich, sollte ein Vorprojekt durchgeführt werden. Die Kosten dafür bewegen sich etwa im Bereich des Aufwandes für die Migration von Windows 3.11/95/98 auf Windows NT 4.0. Technisch weitaus aufwändiger stellt sich allerdings die Integration einer vorhandenen Exchange 5.5-Umgebung über Exchange 2003 in die ADS dar: Hier müssen zwei Systeme mit unterschiedlichen Daten integriert werden. Weniger aufwändig wird es beim Einsatz von Lotus Notes, da hier eine Integration in die ADS auf absehbare Zeit nicht vorgesehen ist.

Der organisatorische Aufwand, der mit der Migration der Benutzerverwaltung von Windows NT 4.0 Domains in Richtung Active Directory verbunden ist, ist dann wiederum höher: Entscheidungen zur Homogenisierung mit Systemen zum Ressourcenmanagement wie beispielsweise Personalwesen, Asset Management und SAP nehmen zwar wenig Zeit ein, benötigen in der Regel aber lange Laufzeiten. Viel Zeit und Energie beanspruchen auch international übergreifende Abstimmungsprozesse.

Kommen wir nun zur Phase 2, dem Design der Active-Directory-Struktur. Dabei lautet die wichtigste Regel jeder AD-Topologie wie dieser Artikel: „Keep IT Simple“. Aus diesem Grund stellt eine einzige AD-Domain in einem Tree oder in einem Forest (siehe dazu auch die Erläuterungen im Kasten auf dieser Seite) in der Regel das optimale Design dar. Viele Fälle, in denen bei Windows NT eigene Domains notwendig waren, lassen sich im AD durch die Organisationseinheiten abbilden. Da der Ansatz mit mehreren Forests vermieden werden soll, stehen dann entweder das Domain-, das Tree- oder das Forest-Modell zur Auswahl. Das Domain-Modell benutzt eine einzige Domain für das komplette Unternehmen und wird mit einer OU-Struktur (Organisational Units) kombiniert, die sich an den geografischen Verhältnissen orientiert. Die Vorteile dieser Vorgehensweise liegen in der zentralen Administration der Sicherheitsrichtlinien (Policies), während über die OU-Struktur eine dezentrale Administration möglich ist. Zudem erweist sich dieses Modell als extrem flexibel, was sich insbesondere bei einer zukünftigen Reorganisation, Akquisition oder Fusion auszahlen wird. So lassen sich beispielsweise einzelne

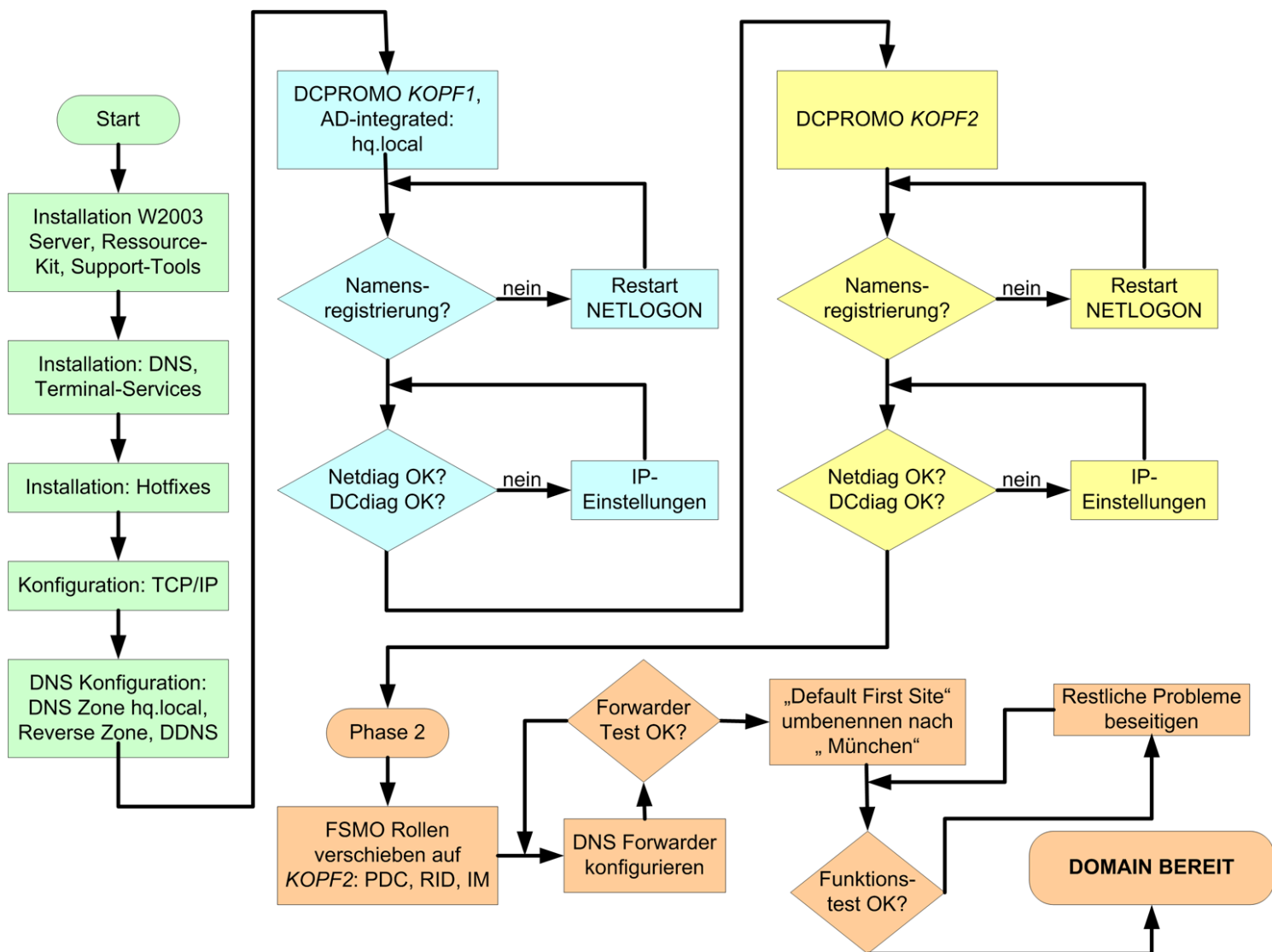


Bild 2. Implementierung des Active Directory: Soll eine separate Wurzel-Domain betrieben werden, so muss diese wie in diesem Ablaufplan gezeigt im ersten Schritt aufgesetzt werden (Quelle: Schmidt's Login).

Objekte (etwa Benutzer) innerhalb der Strukturen beliebig verschieben. Das Domain-Modell führt auch dazu, dass keine Global Catalog Server benötigt werden, da jeder DC alle Objekte repliziert bekommt. Zudem erfordert eine Domain nur einen Namen.

Zu den Nachteilen dieses Modells gehört es, dass sich durch die Zentralisierung der Policies in den Unternehmensbereichen und Niederlassungen oft niemand mehr verantwortlich fühlt. Zudem ist es mit nur einer Domain nicht möglich, unterschiedlichen Sicherheitsanforderungen durch multiple Passwort-Richtlinien (Account Policies) Rechnung zu tragen. Bei großen Domains kommen die entsprechend hohen Hardware-Anforderungen an die Domain-Controller hinzu. Schließlich führt die Verwendung nur einer Domain zu einer ineffektiven Verwendung der WAN-Verbindungen,

da jedes Objekt und jede Objekt-Änderung an jeden DC übermittelt werden muss. Das Tree-Modell erzeugt hingegen aus allen Domains einen einzigen Tree mit fortlaufendem Namensraum. Die Wurzel-Domain, die nicht gelöscht werden kann, fungiert dabei als Platzhalter für die Wurzel des Trees und für unternehmensweite Ressourcen. Jeder Standort beziehungsweise Unternehmensbereich wird dabei durch eine so genannte „First-Level Domain“ repräsentiert. Einer der Vorteile eines solchen Tree-Modells besteht darin, dass eine exakte Abbildung der Unternehmensstruktur im Namensraum entsteht. So finden Benutzer und Administratoren eine gewohnte Umgebung vor, und die Unternehmensbereiche haben die komplette Verfügungsgewalt über ihre eigenen Domains. Die dezentrale Administration auf der Domain-Ebene ermöglicht zudem die Einrichtung und Ver-

waltung individueller GPOs und Passwort-Policies für jede einzelne Domain. Auch die anderen Vorteile des Domain-Modells werden durch ein Tree-Modell erfüllt: So besitzen alle DCs nur von einem Teil der Objekte des Forests ein komplettes Replica, so dass die Hardwareanforderungen an die DCs geringer werden. Auch die Belastung der WAN-Verbindungen wird so spürbar reduziert und Logons laufen schneller ab. Gegen das Tree-Modell spricht der hohe Anpassungsaufwand im Falle einer Reorganisation des Unternehmens. Benutzer- und Ressourcenverschiebungen zwischen Unternehmensbereichen sind ebenfalls nicht einfach. Falls Domains an mehreren Standorten verfügbar sein müssen, erfordert dies die lokale Installation von zusätzlichen DCs dieser Domains. Und obwohl gegenüber dem Domain-Modell verbessert, ist das Tree-Modell hinsichtlich der WAN-Belas-

tung nicht optimiert; hierzu bedarf es dann der Definition von Sites (Standorten).

Das Forest-Modell schließlich stellt eine Variante des Tree-Modells dar, sodass hier praktisch alle Vor- und Nachteile des Tree-Modells ebenfalls gelten. Der wesentliche Unterschied bei diesem Modell besteht darin, dass der Namensraum nicht fortlaufend ist und auch nicht sein kann. Die erste Domain im Forest arbeitet auch hier als Wurzel-Domain. Ein großer Vorteil beim Einsatz dieses Modells entsteht daraus, dass alle Unternehmensbereiche ihren bisher verwendeten Namensraum weiter benutzen und trotzdem in einem gemeinsamen Forest integriert sein können. Allerdings erfordert das Forest-Modell einen Global Catalog. Tiefere LDAP-Abfragen müssen an einen GC-Server gerichtet werden und nicht an einen DC, da ansonsten zum Beispiel eine Abfrage nach einer Ressource in „AU.LOCAL“, die an einen DC in KA.LOCAL gerichtet wird, ins Leere verlaufen würde. In den meisten Fällen entscheiden sich Unternehmen schon während der Vorstudien für das Tree-Modell mit einer zusätzlichen Wurzel-Domain. Gründe dafür sind die Zufriedenheit mit der bestehenden Domain-Struktur und der einfache Migrationsweg per In-Place-Upgrade. Zudem ist eine Restrukturierung später immer noch möglich und wesentlich leichter.

In der dritten Phase geht es nun um die eigentliche Implementierung des Active Directory. Soll eine separate Wurzel-Domain betrieben werden, so muss diese als erste aufgesetzt werden. Daran anschließend kann dann die erste NT-Domain in eine AD-Domain migriert werden. Für alle anderen NT-Domains läuft die Migration zur AD-Domain analog, wobei als Richtwert für den Aufwand etwa ein bis zwei Tage pro Domain gelten. Das Hauptproblem liegt darin, die Verantwortlichen davon zu überzeugen, dass die eigentliche Migration sehr einfach ist.

Nun folgt mit der vierten Phase die Umstellung der Workstations. Bis zu diesem Moment ist die ganze AD-Migration für alle Anwender komplett unsichtbar. Doch um die Möglichkeiten des AD anwenden zu können, müssen die Windows-2000- und -XP-Workstations überhaupt bemerken, dass ein Active Directory vorhanden ist. Dafür genügt die Anpassung folgender Einstellung:

DNS-Server = Domain-Controller des AD

Dies ist sehr einfach, wenn die Einstellungen per DHCP vergeben werden. Dabei

muss das primäre DNS-Suffix nicht geändert werden, wenn die neuen DNS-Server in der Lage sind, beispielsweise durch Weiterleitung auch die bisherige DNS-Zone aufzulösen. Wenn die Windows-Rechner nach dieser Umstellung beim Booten das AD entdecken, sind sie erst nach einem weiteren Boot-Vorgang vollständige Mitglieder des Active Directory und können alle Möglichkeiten nutzen.

Abschließend soll hier noch die zuvor erwähnte Vorstudie zum Migrationsweg erläutert werden. Grundsätzlich existieren zwei Ansätze, um ein Windows NT-Netzwerk nach Windows 2003 Active Directory (AD) zu migrieren: Ein In-Place-Upgrade und die Domain-Restrukturierung, auch Konsolidierung genannt. Die Entscheidung für einen dieser Ansätze oder für eine Kombination der beiden Vorgehensweisen hat große Auswirkung auf den Betrieb des migrierten Netzes.

Microsoft selbst nennt das In-Place-Upgrade das „einfachste Verfahren mit geringstem Risiko“ zur Schaffung einer AD-Struktur, da es existierende Domains, deren User und Computer Accounts sowie alle Security-Gruppen beibehält. Home-Shares, LOGON-Scripts, die Security IDs (SIDs) und Zugriffsrechte auf alle Ressourcen bleiben bei diesem Verfahren ebenfalls erhalten. Es können jedoch Schwierigkeiten entstehen, falls die Windows NT-Struktur aus Ressource- und Account-Domains bestand. Dies stellt zwar kein Problem für User-basierende Policies dar, verkompliziert aber die Verwendung von Group Policy Objekten (GPOs), da während des LOGON auf GPOs aus der Ressource Domain zugegriffen werden muss. Zudem muss man berücksichtigen, dass eventuell vorhandene Windows NT Policies (NTconfig.POL) auch bei Windows-2000/XP-Workstations Anwendung finden und sich nachträglich nur mit großem Aufwand entfernen lassen. Alle Accounts befinden sich nach dem Upgrade noch nicht in OUs, sondern in den Ordnern „Computers“ und „Users“ und müssen nachträglich verschoben werden.

Ist die migrierte Domain in den „Native Mode“ geschaltet, so lässt sich die vorhandene und von Windows NT übernommene Domain-Struktur mittels Microsoft Active Directory Migration Tool (ADMT) oder einem Tool der Firma NetIQ sehr einfach konsolidieren. Das Verschieben von Accounts innerhalb eines Forests zwischen zwei „native Mode“-Domains funktioniert transparent unter Verwendung der SID-History. Das bedeutet, dass die SID dabei erhalten bleibt. Auf diese Weise lassen sich dann nicht mehr benötigte Domains nach

einem In-Place-Upgrade bequem restrukturieren.

Die Alternative zum In-Place-Upgrade besteht darin, eine neue Domain- und OU-Struktur aufzusetzen und mittels ADMT die User und Computer Accounts aus den vorhandenen Domains zu importieren. Diese Domain-Restrukturierung hat folgende Vorteile gegenüber dem In-Place Upgrade:

- Keine Seiteneffekte durch vorhandene NT4 Policies.
- Erstellung und Test von GPOs, bevor produktive User und Computer migriert werden.
- Die importierten Accounts werden direkt in ihren OUs angelegt.
- Die neue Domain-Struktur ist unabhängig von den vorhandenen Strukturen.

Allerdings existieren auch hier eine ganze Reihe von Nachteilen:

- Account-Konflikte: Während der Restrukturierung kann sich durch das Zusammenlegen mehrerer Domains die Notwendigkeit ergeben, User Accounts umzubenennen.
- Neue SIDs: Accounts erhalten generell eine neue SID, alle Zugriffsrechte und ACLs müssen neu gesetzt werden. Ein größeres Problem stellt dies für Ressourcen auf Systemen dar, die nicht unter Windows sondern beispielsweise unter Unix oder VMS betrieben werden.
- Aufwand: Das Umschalten von der alten in die neue Umgebung bedarf sorgfältiger Planung.

Deshalb sollte man unbedingt prüfen, ob man nicht am sichersten und am leichtesten zum angestrebten Ergebnis kommt, wenn eine Kombination aus beiden Verfahren eingesetzt wird. Das bedeutet, dass zuerst ein In-Place-Upgrade aller Domains in einen gemeinsamen Forest durchgeführt wird und daran anschließend eine Restrukturierung folgt. Dieser Ansatz ermöglicht es dann auch, das Active Directory mit minimalem Aufwand in Betrieb zu nehmen. Alle Accounts behalten dabei ihre SID und ACLs bleiben unverändert: Die Restrukturierung kann dann die SID-History verwenden. (fms)

Der Autor

Der Autor dieses Beitrags ist Roland Lötze-
rich, der als Geschäftsführer bei der Firma
Schmidt's LOGIN tätig ist.