Migration von Windows NT 4-Domänen

Die sieben wichtigsten Punkte

Die Einführung von Windows 2000 verlangt eine Überarbeitung der gesamten IT-Struktur. Mit einem schlichten Upgrade ist es nicht getan.

Windows 2000 ist weit mehr als eine neue Version von Windows NT. Es stellt eine umfassende Weiterentwicklung dieses Betriebssystems dar, bei der praktisch alle Funktionen erweitert und verbessert werden - und viele neue Leistungsmerkmale gerade für das Enterprise Computing hinzukommen. Das bedeutet aber auch, dass sich die Einführung von Windows 2000 nicht immer auf ein simples Upgrade beschränken kann. Das wird in manchen Bereichen sicherlich so sein.

In kleineren Netzwerken, bei wenigen Anwendungsservern und vor allem bei einer kleinen Anzahl von NT-Workstations lässt sich der Schritt zu Windows 2000 sehr einfach durchführen. Bei Domänencontrollern in größeren Netzwerken gilt das aber nicht. Um die Vorbereitung auf die Migration zu Windows 2000 zu erleichtern, haben wir nachfolgend die sieben kritischen Erfolgsfaktoren zusammengefasst, die bei der Planung der Migration beachtet werden sollten.

Die Planungsbereiche

Bei der Planung für Windows 2000 lassen sich sieben zentrale Planungsbereiche isolieren:

Actlve Directory:

Der zentrale neue Verzeichnisdienst

Sicherheit:

Das Active Directory mit der Möglichkeit einer differenzierteren Zuweisung von Berechtigungen muss ebenso wie neue Technologien, so zum Beispiel das Encrypting File System, bei der Planung berücksichtigt werden

Administration von Clients:

Clients

Hier gibt es durch die IntelliMrror-Technologien viele neue Möglichkeiten
Netzwerk: Die größere Rolle von DNS, verteilte Dateisysteme und Erweiterungen bei TCP/IP machen hier erweiterte Konzepte erforderlich

PKI:

Public Key-Infrastrukturen werden eine zunehmend wichtige Rolle spielen

Namensregeln:

Windows 2000 wird mit NetBIOS-, DNS- und LDAP-Namen mehrere verschiedene Namenskonzepte unterstützen

Integration:

Die Rolle von Windows 2000 als Teil der gesamten lT-Infrastruktur muss definiert werden

Darüber hinaus muss dann auch noch der Ablauf von Migrationsplanung und Migration sowie des späteren Betriebs von Windows 2000 definiert werden.

Ganzheitliche Planung

Der wohl wichtigste Erfolgsfaktor beim Schritt in Richtung Windows 2000 ist, dass mit einem ,,ganzheitlichen" Ansatz gearbeitet wird. In vielen Unternehmen gibt es in der lT mehrere Bereiche. Ein Bereich ist für das Netzwerk und die Verkabelung, einer für den Betrieb von Servern, einer für Benutzerverwaltung und Helpdesk verantwortlich. Und jeder dieser Bereiche ist von der Umstellung auf Windows 2000 betroffen. Zwischen den verschiedenen Planungsbereichen bestehen Abhängigkeiten. So wirkt sich beispielsweise die Struktur von Sites und Domänen im Active Directory massiv auf die Replikationslast im Netzwerk aus.

Ein anderes Beispiel sind die Gruppenrichtlinien. Sie werden als Objekte im Active Directory zugeordnet, steuern aber sowohl Sicherheitseinstellungen als auch die Client-Konfiguration. Für eine erfolgreiche Planung von Windows 2000 sollten die verschiedenen beteiligten Bereiche koordiniert zusammenarbeiten und die vielfältigen Abhängigkeiten der Planungsbereiche untereinander berücksichtigt werden. Das aber setzt voraus, dass alle wichtigen Änderungen bei Windows 2000 gegenüber der Vorgängerversion und ihre Implikationen verstanden wurden. Ganzheitlich heißt aber auch, dass das Projekt nicht nur unter dem Blickwinkel von Windows 2000, sondern der gesamten lT - also gerade auch im Hinblick auf die Integration mit anderen Systemen - betrachtet wird.

Betriebshandbücher

Windows 2000 kann sehr viel mehr als Windows NT. Das zeigt sich beispielsweise daran, dass administrative Berechtigungen nun sehr viel differenzierter festgelegt werden können. Es zeigt sich aber auch am Unterschied zwischen den vergleichsweise einfachen Systemrichtlinien von Windows NT und den komplexen, aber ungleich leistungsfähigeren Gruppen-Richtlinien von Windows 2000. Das bedeutet aber, dass die Konzepte für den Betrieb entsprechend angepasst werden. Im Vergleich zu Windows NT werden Betriebs-Handbücher auch wesentlich wichtiger. Mittlere und größere Netzwerke werden sich ohne solche klaren Richtlinien nicht mehr effizient administrieren lassen.

Das unternehmensweite Projekt

Das Active Directory - oder ein anderer hierarchischer, verteilter Verzeichnis-Dienst wie die NDS - wird der zentrale Baustein von Windows 2000 werden. Ein solcher Verzeichnisdienst kann aber, auch bedingt durch technische Aspekte, nur sinnvoll funktionieren, wenn er zentral für das gesamte Unternehmen geplant wird. Der bei Windows NT gar zu oft zu findende Ansatz, bei dem viele kleine Netzwerke entstehen - im englischen so treffend als ,,grass roots" bezeichnet - verbietet sich bei Windows 2000. Das setzt voraus, dass dieses Projekt nicht nur die IT-Fachbereiche koordiniert, sondern sich auch über die unterschiedlichen Standorte und Unternehmensbereiche erstreckt.

Heute Grundlagen schaffen

Um diese Situation nach Möglichkeit überhaupt nicht entstehen zu lassen, ist es auch wichtig, heute bereits Grundlagen zu schaffen. Das betrifft vor allem die Definition und Durchsetzung (!) von einheitlichen Regeln für die Bildung von Domänen schon bei Windows NT. Sie sollten sich, soweit hier noch neue Domänen geschaffen oder Änderungen vorgenommen werden, bereits an Windows 2000 orientieren. Die Migration zu Windows 2000 ist zwar in relativ flexibler Form durchführbar. Wichtig ist aber dennoch, dass nicht heute Entwicklungen laufen, die später unnötige Arbeit schaffen.

Neue Möglichkeiten nutzen

Auch wenn Microsoft es gerne so verkauft:

Die meisten Unternehmen werden nicht glücklich werden, wenn sie sich auf ein einfaches Upgrade von Domänen beschränken. Der Schritt zu Windows 2000 zahlt sich nur dann wirklich aus, wenn auch die neuen Möglichkeiten des Betriebssystems genutzt werden. Und das bedeutet zwangsläufig einen hohen konzeptionellen Aufwand, da sich ohne ihn die Gruppenrichtlinien, Public Key-Infrastrukturen oder der Intellimirror-Ansatz nicht effizient einführen und dauerhaft nutzen lassen. Wer aber auf diesen Aufwand - die eigentliche Migration - verzichtet und sich auf ein simples Upgrade beschränkt, läuft Gefahr, sowohl später aufwendig Fehler in der Administration korrigieren zu müssen als auch einen viel zu geringen Nutzen aus dieser Investition zu ziehen.

Schnelligkeit

Windows 2000 unterstützt beim Active Directory sowohl einen nativen als auch einen gemischten Modus. Im nativen Modus gibt es nur Windows 2000-Domänen-controller, während im zweiten Modus auch Sicherungsdomänencontroller unter Windows NT 3.51/4.0 betrieben werden können. Der schnelle Schritt zum nativen Modus ist sinnvoll, damit sich die Zahl der Domänencontroller verringert und man unnötige Last im Netzwerk durch die Kommunikation sowohl zwischen Windows 2000-Domänencontrollern als auch zwischen Windows NT-Domänencontrollern vermeidet.

Ausreichend Vorlauf

Wer nicht rechtzeitig mit dem Migrationsprojekt zu Windows 2000 beginnt, wird dafür entweder in Form von Planungsfehlern oder erheblichen zeitlichen Verschiebungen im Projekt bezahlen.

Windows 2000 ist komplex

Das Sammeln von Know-how, die Evaluation von Windows 2000, die Planung der Migration inklusive Vorbereitung und Test sowie die eigentliche Durchführung der Migration brauchen viel Zeit. Windows 2000 ist, wie schon eingangs erwähnt, nicht einfach nur eine neue Version von Windows NT, sondern ein weitgehend neues Betriebssystem. Um die komplexen Zusammenhänge im System und die neuen Technologien zu verstehen, braucht es Zeit. Migrationsprojekte in größeren Netzwerken werden dabei kaum unter einem Jahr zu bewerkstelligen sein, selbst wenn ausreichend Ressourcen bereitstehen.

Windows 2000 ist ein Betriebssystem, das eine Vielzahl von Funktionen im Enterprise-Bereich bringt. Es muss aber auch entsprechend behandelt werden. Die Bedeutung von Server-Betriebssystemen wie Windows 2000 ist heute ,,mission critical". Deshalb muss ein Migrationsprojekt von Windows NT zu Windows 2000 auch mit dem gleichen Fokus und Anspruch betrachtet werden wie ein komplexes Einführungsprojekt im Mainframe-Bereich. Und deshalb muss die konzeptionelle Vorarbeit ebenso stimmen wie der zeitliche Rahmen. Nur dann wird der Schritt zu Windows 2000 von Erfolg gekrönt sein.

Migration im Detail

Die Migration von Windows NT 4-Domänen hat gegenüber einer kompletten Neuinstallation den unschätzbaren Vorteil, daß alle Benutzer- und Gruppenkonten mit den ihnen erteilten Zugriffsberechtigungen auf Ressourcen erhalten bleiben. Besteht das Netzwerk einer Organisation aus Windows NT 4-Domänen muß in der Phase der Grobplanung auch die grundsätzliche Migrationsstrategie festgelegt werden. Es werden in den nächsten Abschnitten folgende Punkte besprochen:

?? Migration einer einzelnen Domäne
?? Migration eines Master- oder Multiple-Master-Domänenmodells

Der einfachste Fall, ist die Migration einer einzelnen NT4-Domäne. Wenn festgelegt wurde, daß das Active Directory nach der Migration ebenfalls nur aus einer Domäne bestehen soll, wird eben einfach die vorhandene NT4-Domäne zu Windows 2000 aktualisiert. Die wichtigsten Punkte, die hierbei berücksichtigt werden müssen sind die folgenden:

?? Der PDC ist der erste Domänencontroller, der zu Windows 2000 aktualisiert wird.
?? Es sollte aus Sicherheitsgründen vorher ein BDC manuell aktualisiert und anschließend aus dem Netz genommen werden. Gibt es Probleme bei der Migration des PDC, kann der BDC zum PDC hochgestuft und so die NT4-Domäne wiederhergestellt werden.
?? Nach dem PDC werden schrittweise alle BDCs aktualisiert.
?? Wenn alle Domänencontroller zu Windows 2000 migriert sind, muß die Domäne vom gemischten in den nativen Modus geschaltet werden, damit auch die ehemaligen BDC in die Lage versetzt werden, neue Objekte im Active Directory zu erstellen.
?? Anschließend werden eventuell vorhandene Windows NT Member Server zu Windows 2000 aktualisiert und in das Active Directory integriert.
?? Der letzte Schritt besteht aus der Migration der Clientrechner zu Windows 2000 Professional

Der kritische Faktor bei der stufenweise Migration einer Windows NT 4.0 Domäne ist ohne Zweifel der ehemalige PDC. Solange die Domäne noch im mixed mode arbeitet, können auf den ehemaligen BDC keine neuen Objekte angelegt werden. Der ehemalige PDC kann nämlich nach wie vor als einziger auf den RID-Pool der Domäne zugreifen, um neuen Objekten Security-IDs zuzuweisen. Folgende Hinweise sollte man daher während der Umstellungsphase beherzigen:

?? Der PDC sollte erst dann migriert werden, wenn er eine längere Zeit stabil gelaufen ist, damit er in der Umstellungsphase möglichst nicht ausfällt.
?? Hat man mehrere Domänencontroller mit unterschiedlicher Hardware, sollte man tunlichst denjenigen BDC mit der zuverlässigsten Hardware zum PDC heraufstufen und diesen migrieren
?? Absolute Pflicht sind häufige Backups des PDC

Vor der Planung der Migration eines Master-Domänenmodells muß man sich darüber im klaren sein, wie das Active Directory strukturiert sein soll. Die Planung des Active Directory sollte losgelöst von der vorhandenen Domänenstruktur erfolgen, damit Probleme und Kompromisse, mit denen man im Zusammenhang mit der NT4 Domänenstruktur zu leben gelernt hat, nicht einfach ohne Hinterfragen in das neue Netzwerk übernommen werden und dort die gleichen Schwierigkeiten bereiten. Deshalb ist es auch sehr wichtig, in der Phase der Bedarfsanalyse technologieneutrale Ziele zu formulieren.

Die Migration eines Master-Domänenmodells beginnt immer mit der Umstellung der Masterdomäne. Für die Ressourcendomänen ändert sich gar nichts, denn ihre Vertrauensbeziehungen mit der Masterdomäne existieren nach wie vor.

Ist die Masterdomäne komplett migriert, können auch die Ressourcendomänen migriert werden. Als Voraussetzung darf allerdings nicht die Erstellung einer korrepondierenden DNS-Domäne mit der entstehenden Active Directory Domäne der Ressourcen-Domäne vergessen werden.

Die Ressourcen-Domänen werden zu neuen Child-Domänen im Active Directory. Die Objekte der Ressourcen (Child)-Domänen könnten jedoch genauso gut in die übergeordnete Hierarchie verschoben werden und somit zu OUs (Organisational Units) werden.

Hinsichtlich der Migration eines Multi-Master-Domänenmodells muß außer der Frage, ob die Ressourcendomänen konsolidiert werden sollen, auch noch geklärt werden, auf welche Weise die Masterdomänen in das Active Directory integriert werden.

Es bestehen grundsätzlich eine ganze Reihe von Möglichkeiten:

?? Alle Masterdomänen werden zu einer einzigen Active-Directory Domäne konsolidiert
?? Die Masterdomänen bilden keinen zusammenhängenden Namensraum, sondern werden als eigenständige Domänenbäume innerhalb eines gemeinsamen Forests ausgelegt.
?? Eine der Masterdomänen wird die neue Root-Domain, die übrigen werden zu untergeordneten Domänen.

Welches Modell letztendlich realisiert wird, ist einzig und allein von den in der Bedarfsanalyse definierten Zielen einer Organisation und der sich daraus ergebenden Struktur des Active Directory abhängig. Windows 2000 jedenfalls ist so flexibel, daß jede nur denkbare Alternative realisiert werden kann.

Bei der Aktualisierung Windows NT 4 zu Windows 2000 werden die Windows NT 4 Kontenrichtlinien nicht übernommen. Wird die Windows NT 4 Domäne zur untergeordneten Domäne, werden die Richtlinien der Root-Domain übernommen. Bildet die Windows NT 4-Domäne hingegen einen eigenen Domänenbaum, werden die Standardeinstellungen von Windows 2000 angewendet. Dies muß in der Planung der Migration ebenfalls berücksichtigt werden. Ohnehin sollte man die bestehenden Kontenrichtlinien im Rahmen der Bearbeitung der Sicherheitseinstellungen kritisch überdenken, da Windows 2000 wesentlich ausgefeiltere Konfigurationsmöglichkeiten bietet als Windows NT 4.0.

Windows 2000 als PDC

Falls der Schritt zum Active Directory erfolgt, muß zunächst der primäre Domänencontroller migriert werden. Das ist eine Konsequenz des Umgangs mit RIDs. Ein solcher Relativer Identifier identifiziert Objekte im Verzeichnis eindeutig. Er wird auf Basis des SID (Security Identifier) der Domäne, des Servers oder der Workstation, auf der ein Konto angelegt wird, definiert. Der RID besteht immer aus einem Teil der SID und zusätzlichen Informationen. Der RID muß ebenso wie die SID eindeutig sein. Der SID muß eindeutig sein, damit es unterschiedliche RIDs geben kann. Die RIDs wiederum müssen eindeutig sein, weil über sie die Benutzerrechte zugeordnet werden. Wären sie nicht eindeutig, so könnt es auch keine eindeutige Zuordnung von Benutzerrechten geben. Bisher gab es keine hohen Anforderungen an der Eindeutigkeit der SID bzw. RID, da alle Änderungen ja sowieso nur auf dem PDC durchgeführt werden konnten. Mit Active Directory und der Multi-Master Replikation wird sich das grundlegend ändern, da nun jeder DC in der Lage ist, Berechtigungsänderungen im Verzeichnis durchzuführen.

Bei manchen Operationen ist ein solches Konzept aber nur mit sehr großem Aufwand zu realisieren. Hier macht es dann eher Sinn, diese Operationen in Form von Single-Master-Replikationen vorzunehmen. Die Änderung kann also nur bei einem System erfolgen und wird dann auf alle anderen Systeme repliziert.

Das erleichtert nicht nur die Implementierung, sondern schützt die Umgebung vor unnötigem Netzwerkverkehr und zusätzlicher Last, die für die Lösung von Konflikten entstehen würde.

Ein gutes Beispiel hierfür sind Änderungen im Schema. Solche Schemaänderungen sind folgenreiche Operationen, da sie nicht mehr rückgängig gemacht werden können. Sie können allenfalls deaktiviert werden. Deshalb werden diese Operationen nicht sehr häufig vorgenommen. Sie dürfen auch nur von einem sehr kleinen Kreis berechtigter Administratoren vorgenommen werden. Für solche Operationen wird das Multiple-Master-Replikationskonzept umgangen. Die Änderungen können nur auf einem ganz speziellen Domänencontroller vorgenommen werden.

Die Operationen, für die solche Einschränkungen gelten, sind die sogenannten Flexible Single Master Operations (FSMO). Der Name macht deutlich, daß die Änderungen nur an einem dedizierten Domänencontroller vorgenommen werden kann. Er besagt aber auch, daß die Rolle des sogenannten FSMQ-Rollenbesitzers von einer anderen Maschine zur nächsten transferiert werden kann.

Das Wechseln der Rolle macht in den meisten Fällen aber nur dann Sinn, wenn mit der Rolle auch die Daten überspielt werden können. Deshalb versuchen die Administrationswerkzeuge immer, die Rolle im Einvernehmen zwischen den beiden Domänencontrollern zu transferieren. Sollte jedoch eine Maschine, die ein FSMO-Rollenbesitzer ist, für immer verloren oder für längere Zeit ausgefallen sein, kann diese Rolle auch ohne einen solchen Abstimmungsprozess von einer anderen Maschine übernommen werden. Damit kann diese Rolle auch transferiert werden, wenn ein FSMO-Rollenbesitzer nicht mehr verfügbar ist.

Im AD von Windows 2000 gibt es fünf verschiedene FSMO-Rollen. Zwei davon haben einen Gültigkeitsbereich für den gesamten Forest. Es kann also nur einen FSMO-Rollenbesitzer für die Operation im gesamten Forest geben. Die drei anderen FSMO-Operationen haben einen Gültigkeitsbereich für die Domäne.

Ein Domänencontroller kann der Rollenbesitzer für mehrere FSMOs sein. Die FSMOs können aber auch an mehrere Maschinen verteilt werden.

Die FSMOs mit Gültigkeitsbereich für den gesamten Forest sind:

?? Schema Master FSMO:

Das ist die einzige Maschine, auf der Ergänzungen im Schema vorgenommen werden können.

?? Domain Naming FSMO:

Die Maschine, die diese Rolle übernimmt, stellt sicher, daß beim Hinzufügen einer Domäne zu einem existierenden Forest ein Domänenname verwendet wird, der noch nicht vorhanden ist. Gerade an diesen Beispielen wird deutlich, daß es sich bei FSMO-Rollenbesitzern wirklich nur um Systeme handelt, die in Sonderfällen aktiv werden. Daher macht es Sinn, hier mit Single-Master-Operationen zu arbeiten, statt komplexe und aufwendige Abstimmungsmechanismen in einem Multi-Master-Modell zu entwickeln.

Die domänenweiten FSMOs sind:

?? RID Pool Owner FSMO:

Da in Windows 2000 neue Objekte auf jedem Domänencontroller erzeugt werden können, muß bei neuen Security Principals (Benutzern, Gruppen oder Windows NT, W2K-Benutzerkonten) sichergestellt werden, daß die relative ID (RID) des neuen Objekts eindeutig in der Domäne ist und nicht bereits von einem anderen Domänencontroller verwendet wurde, bevor das neue Objekt repliziert wurde. Das wird gelöst, indem ein RID Pool Owner FSMO eben RID-Pools erzeugt, die immer genau 500 RIDs beinhalten. Dieser Pool wird dann einem Domänencontroller zur Erzeugung neuer Objekte übertragen. Wenn ein Domänencontroller bereits eine große Anzahl RIDs (80%) verbraucht hat, beantragt er bei dem RID Pool Owner FSMO einfach einen neuen Pool.

?? PDC Emulator FSMO:

Der PDC Emulator FSMO wird benötigt, um älteren Clients, die mit dem PDC von Windows NT direkt kommunizieren wollen, einen solchen bereitzustellen. Dieses System wird nur für Zugriffe benötigt, die direkt einen PDC adressieren. Beispielsweise registriert der PDC Emulator einen PDC-Eintrag in WINS solange WINS noch genutzt wird. Der PDC Emulator wird auch für Optimierungen bei Kennwort-Änderungen verwendet. Das ist immer dann der Fall, wenn ein Anwender sein Kennwort geändert hat, dieses aber noch nicht überallhin repliziert wurde.

?? Infrastructure FSMO:

Dieser dedizierte Domänencontroller hält sich auf dem Laufenden, wo sich Objekte befinden, die von seiner Domäne in eine andere verschoben wurden. Dies ist wichtig, um zum Beispiel Gruppenangehörigkeiten immer korrekt aufzulösen. Wenn nun ein Windows NT 4.0-Domänencontroller die Funktion eines PDC übernehmen würde, wäre dieser schlicht nicht in der Lage, die entsprechenden Informationen bereitzustellen, denn dieses System kennt keine RID-Pools. Daher muß als Ergebnis zunächst der primäre Domänencontroller migriert werden.

Dieser erste Domänencontroller wird standardmäßig im sogenannten Mixed-Mode betrieben. Das bedeutet, daß er alle Schnittstellen für die Kompatibilität mit bisherigen Windows NT Domänencontrollern bereitstellt. Dazu zählen folgende Eigenschaften:

?? Das System stellt die Schnittstellen auf der Ebene von NetBIOS bereit, die auch von Windows NT genutzt werden. Das bedeutet beispielsweise, daß sich das System je nach Konfiguration über NetBIOS Broadcasts bekannt macht. Es bedeutet aber vor allem, daß der Browser-Dienst (Computer-Suchdienst) voll unterstützt wird. Das ist nicht vom Betrieb im mixed mode abhängig.
?? Für die Kommunikation zwischen Domänencontrollern werden bisher die sicheren Kommunikationskanäle auf Basis des NTLM und SMB verwendet. Diese sind ab SP4 zwar sehr sicher (wenn über die Registry aktiviert), werden bei Windows 2000 aber durch einen Mechanismus ersetzt, der auf der Kerberos-Sicherheit basiert.
?? WINS wird weiterhin unterstützt. Allerdings ist die Unterstützung dieses Mechanismus, wie viele NetBIOS basierende Funktionen, auch erforderlich, wenn nicht alle Clients auf Windows 2000 migriert wurden oder entsprechende Client-Software eingesetzt wird. Das ist allerdings nicht vom Betrieb im mixed mode abhängig.
?? Die Replikation der SAM erfolgt nach dem gleichen Mechanismus wie bisher. Der Windows 2000 Domänencontroller verhält sich aus der Sicht der BDC wie ein PDC unter Windows NT 4.0.
?? Es gibt keine universellen Gruppen und auch keine Schachtelung von Gruppen über die Möglichkeiten der globalen Gruppen und lokalen Gruppen hinaus. Diese werden nur im Native Mode unterstützt.

Typische Business-Ziele bei einer NT zu Win2K Migration

Ziel	Feature	Vorteile
Bessere Verwaltungsmöglichkeiten	Transitive Kerberos Trusts	Reduziert den Aufwand für die explizite Konfiguration von Trusts
	Active Directory Ressourcenlokation und –Administration	Active Directory bietet eine einheitliche Schnittstelle für die Administration, der Ermittlung von Personen und Ressourcen in einer Enterprise-Umgebung
	Active Directory Organizational Units (OU)	Administrative Rechte können auf eine OU delegiert werden
	Active Directory Sicherheitsgruppen	Windows 2000 bietet eine höhere Anzahl an Gruppen zur Rechtesteuerung
Bessere Skalierbarkeit	64-Bit Speicherarchitektur	Windows 2000 ermöglicht die Nutzung von bis zu 32 GB Speicher (RAM)
	Active Directory Skalierbarkeit	Active Directory skaliert bis zu 10 Millionen Objekte im AD
	Kerberos Authentifikation	Erhöht die Authentifizierungs-geschwindigkeit und verringert die Serverlast
	MMC	Vereinheitlicht alle Managementtools
Erhöhte Sicherheit	Group Policy	Group-Policies erhöhen die Sicherheit und bieten granularere Delegation von Einschränkungen
	Security Configuration Tool Set (SCTS)	SCTS ist ein Set von MMC Snap-Ins, welche die Sicherheitsrichtlinien benutzerdefiniert erweitern lassen
	Setup	Windows 2000 wird mit höheren Standard-Sicherheitseinstellungen ausgeliefert
Erhöhte Verfügbarkeit	Active Directory Mulit-Master-Replikation	Dies erhöht die Verfügbarkeit der DCs, wenn ein System ausfällt

Typische Ziele für eine Migration

Ziel	Bedeutung für den Migrations-Prozess
Minimale Störung der produktiven Umgebung	Benutzer-Zugriff auf Daten und Ressourcen sollte während und nach der Migration verfügbar sein Benutzer-Zugriff auf Applikationen sollte während und nach der Migration möglich sein Die Benutzerumgebung des Benutzers sollte während und nach der Migration verfügbar sein
Minimaler administrativer Overhead	Die Migration der Benutzer sollte möglichst ohne Änderungen erfolgen Benutzer sollten ihre alten Passwörter weiter verwenden können Die Notwendigkeit der manuellen Administration an den Workstations sollte vermieden werden Es sollte vermieden werden, neue Berechtigungen für Ressourcen vergeben zu müssen
Schnelle Erfolge	Die Migration sollte schnellstmöglich erfolgen
System-Sicherheit	Die Sicherheitsrichtlinien sollten in Abwägung des zumutbaren und erforderlichen umgesetzt werden

Migrations-Konzepte

Es existieren zwei Konzepte für die erforderliche Migration:

?? Domain Update und
?? Domain Restrukturierung

Domain Update und Domain Restrukturierung schließen sich nicht gegenseitig aus. Manche Unternehmen führen erst ein Domain Update durch und restrukturieren dann die Domäne.

Domain Update

Das Update zu Windows 2000 ist das mit am wenigsten Risiken verbundene Vorhaben.

Ein Domain Upgrade meint das Update der installierten Betriebssystemsoftware auf eine neue Version. Dies betrifft alle BDC, den PDC und die jeweiligen Member Server.

Das Update des PDC auf Windows 2000 ist der erste Schritt in einer Kette von Migrationsschritten.

Bedeutung des Domain Updates

Das Domain Update ist wie bereits erwähnt, die einfachste und gefahrloseste Art des Updates. Nachfolgend werden die einzelnen Schritte bei einem Domain Update besprochen:

Einrichten von Diensten für den automatischen Start

Während der Installation von AD werden die folgenden Dienste für den automatischen Start konfiguriert:

RPCLocator, der verteilten Anwendungen die Verwendung des RPC Namensdienstes von Microsoft ermöglicht. Der RPC-Locator Dienst verwaltet die Datenbank des RPC-Namensdienstes.

Der Anmeldedienst, der den Locator-Algorithmus des Domänencontrollers ausführt. Der Anmeldedienst sorgt des Weiteren für die Erstellung eines SCC zwischen Client und Domänencontroller. Desweiteren registriert er die SRV Einträge im DNS sowie die Unterstützung von LMRepl.

Der KDC-Dienst, der auf einem physisch sicheren Server ausgeführt wird und eine Datenbank mit Konteninformationen zu allen Sicherheitsprincipals im zugehörigen Geltungsbereich enthält.

IsmServ (ISM-Dienst), der Dienst für die e-mail basierte Replikation der Daten zwischen den Standorten. Replikationsdaten werden über SMTP über die Standorte übermittelt. Die SMTP-Komponente wird unter Verwendung von IIS 5.0 eingesetzt.

TrkSvr (Serverdienst zur Überwachung verteilter Verknüpfungen), der auf jedem Domänencontroller einer Domäne ausgeführt wid.

W32Time (verteilter Zeitdienst), über den Uhrzeiten zwischen Windows 2000 Clients und Servern synchronisiert werden. Die Zeitsynchronisation erfolgt automatisch.

DCPROMO

Nach erfolgter Synchronisation der BDC mit dem PDC in der Domäne, kann das Programm DCPROMO auf einem zu Windows 2000 migrierten Domänen-Controller erfolgen. DCPROMO installiert das Active Directory auf dem migrierten Server und evtl. einen neuen DDNS-Server.

Der Assistent zum Installieren von AD erfordert 200 MB Speicherplatz für die Active Directory Datenbank und 50 MB für die ESENT-Transaktionsprotokolldateien. Die Datenbankgrößenanforderungen für die Active Directory Datenbank und die Protokolldateien richten sich nach Anzahl und Typ der Obkete in der Domänendatenbank, die durch die Gesamtstruktur gespeichert werden, wenn der Computer als globaler Katalogserver fungiert.

Windows NT PDC

Während des Migrationsprozesses wird die SAM des PDC in das Active Directory kopiert. Diese Objekte sind die Security Principals (Benutzer-Accounts, Lokale- und Globale Accounts und Computer-Accounts.

Sobald der PDC zum Windows 2000 Domänencontroller migriert wurde, läuft die Domäne im sogenannten Mixed-Mode und bietet Windows 2000 Funktionalitäten aber auch Upgradekompatibilität zu älteren NT Systemen bis V 3.51.

Features:

- ?? Der PDC funktioniert als Windows 2000 Domänencontroller in Win2K Umgebungen
- ?? Der PDC kann weiterhin die SAM mit den BDC abgleichen
- ?? Windows NT und Win9x Clients nutzen den PDC weiterhin als Anmeldeserver
- ?? Wenn der Win2K PDC offline geht und kein anderer Win2K Server verfügbar ist, kann ein vorhandener BDC zum PDC promotet werden.

Der Update Effekt auf die Access Controls

Security Identifiers (SIDs)

Das Windows NT Sicherheitsmodell basiert auf sogenannten SIDs, welche Benutzern, Gruppen, Ressourcen und Trusts in einem Netzwerk zugeordnet sind.

SIDs sind in einer Domäne eindeutig. Doppelte SIDs dürfen nicht vorkommen und kommen auch nicht vor.

Die Struktur einer SID ist immer gleich. Eine SID besteht aus einer Revisions-Nummer wie die sogenannte Authority – die Domäne, und eine variable Anzahl von Zahlen, welche an die SID gehängt werden, die sogenannte RID (Relative Identifier).

Die SID wird in einem NT / Windows 2000 Netzwerk immer dazu benutzt, um einen Benutzer am System mit entsprechenden Berechtigungen, den Zugriff auf die Ressourcen zu gewähren.

Authorization und Security Descriptors

Der Gegensatz zu den SID ist der Security Descriptor für Ressourcen wie Dateien oder Drucker. Ein Security Descriptor beinhaltet eine ACL (Access Control List), welche wiederum ACEs (Access Control Entries) enthält.

Bei einem Upgrade werden die Security Principals und die SIDs nicht verändert, so dass keine Probleme mit den Sicherheitseinstellungen auftreten sollten.

Der Update-Effekt auf die Trusts

DCPROMO installiert die Kerberos-Software. Wenn die Installation durchgeführt wurde, werden die Ticket-Granting Services und die Authentication-Services gestartet. Zwischen den Domänen wird ein Two-Way-transitiver Trust gebildet. Eventuell vorhandene Trusts der NT 4 Domäne bleiben existent, existieren jedoch als explizite One-Way-Trusts ohne transitive Vertrauensstellungen.

Eventuell kopiert der DC der übergeordneten Domäne das Schema und die Konfigurationsinformationen zu der neuen Child-Domain. Wenn diese Informationen repliziert worden sind, ist die upgedatete Domäne ein vollwertiges Mitglied des Active Directories.

Active Directory fähige Clients wie Windows 2000 Professional und Windows 9x, welche die Active Directory Client Software installiert haben, können nun das AD zur Ressourcensuche mit Hilfe des Global Catalog Servers oder manuell durchführen.

Ressourcen sind jedoch nur innerhalb des Forest oder innerhalb der transitiven Trusts sichtbar, wenn folgende Bedingungen erfüllt sind:

- Domänen im Native Modus
- Mixed Mode Domains, wenn alle DCs ubgedatet worden sind
- Mixed Mode Domains, wenn alle DCs mit dem Kerberos oder NTLM Dienst ubgedatet worden sind.

In allen anderen Fällen haben Clients nur Zugriff auf explizite One-Way-Trusts.

Verwendung der NTLM Authentifizierung

Eine NT Workstation authentifiziert sich über das NTLM-Verfahren. In einer Mixed-Mode Domain werden sowohl Kerberos als auch NTLM unterstützt. Die NT Workstation nimmt per NTLM Kontakt zu einem Windows 2000 DC auf. Der DC überprüft die Anmeldung und stellt fest, dass er keinen Bezug zu der Anfrage in der

Datenbank findet. Da es sich in diesem fiktiven Szenario um einen DC in einer Child Domain handelt, wird Kontakt mit der übergeordneten Domäne aufgenommen. Da diese Vertrauensstellungen transitiv sind, gibt es keine Probleme. Der übergeordnete DC überprüft den Benutzernamen und das Kennwort in der SAM und sendet es zurück an den DC in der Child-Domäne.

Der Server erstellt ein Access Token, welches die SID aller Gruppen des Benutzers beinhaltet. Es erstellet dann einen Impersonfikations-Thread im Sicherheits-Kontext des anzumeldenden Benutzers mit Hilfe des Impersonifikations-Tokens und versucht im „Namen“ des Benutzers auf die Ressource zuzugreifen.

Verwendung der Kerberos Authentifizierung

Mit einem vergleichbaren Konzept der NT-Vertrauensstellungen arbeitet auch Kerberos. Hier vertrauen die Benutzer auf den Sicherheitsmechanismus von Kerberos. Server vertrauen Kerberos, wenn der Benutzer eine Authentisierung für die Benutzung des jeweiligen Servers vorweisen kann.

Allerdings findet sich auch der gegenteilige Ansatz bei Kerberos. Kerberos geht davon aus, dass die Stationen im Netzwerk nicht vertrauenswürdig sind. Ein Benutzer muss sich jedes Mal, wenn er auf einen Server zugreift, gegenüber diesem identifizieren. Dazu muss er allerdings keineswegs jedes Mal ein Kennwort eingeben. Vielmehr wird auf verschlüsselte Informationen im Cache seines Servers zugegriffen.

Für die Entwicklung von Kerberos wurden einige grundlegende Regeln aufgestellt:

- Der Benutzer identifiziert sich genau einmal zu Beginn seiner Arbeitssitzung. Dazu wird die normale Anmeldung mit Benutzername und Kennwort verwendet.
- Kennwörter werden niemals im Klartext über das Netzwerk gesendet, sondern immer verschlüsselt.
- Jeder Dienst auf dem Netzwerk besitzt ein Kennwort, das mit ihm assoziiert ist.
- Die einzige Einheit im Netzwerk, der die Kennwörter bekannt sind, ist der Kerberos Authentication Server (KAS).

An zentraler Stelle im Konzept von Kerberos steht der Key Distribution Service (KDS). Dieser besteht wiederum aus drei Elementen:

- Der Kerberos Authentication Server (KAS) ist für die Authentisierung von Benutzern zuständig.
- Der Kerberos Ticket Granting Server (TGS) stellt Tickets für den Zugriff eines authentisierten Benutzers auf einen Dienst aus.
- Die Kerberos-Datenbank enthält die Kennwörter

Dass der Server, auf dem der KDS ausgeführt wird, auch physisch sicher sein muss, versteht sich von selbst. Zwar werden auch hier Kennwörter in verschlüsselter Form gespeichert, dennoch ist er natürlich das sensibelste Element im ganzen Konzept. Windows 2000 wird auf den Domänencontrollern einen solchen KDS als Funktion des Active Directory Service bereitstellen. Die Kerberos-Datenbank wird in den

Verzeichnisdienst von Windows NT integriert, so dass die Datenbankinformationen in der Datenbank des Verzeichnisdienstes von Windows 2000 abgelegt werden.
Wenn sich nun ein Benutzer anmeldet, gibt er zunächst seinen Benutzernamen ein. Dieser wird über das Netzwerk zum KAS gesendet. Sie enthält den Benutzernamen und den Namen des TGS und ist nicht verschlüsselt. Das ist zu diesem Zeitpunkt auch nicht erforderlich, da sie nur zwei Namen enthält. Namen von Benutzern und Diensten müssen für die Kommunikation bekannt sein. Es macht allerdings auch einen Unterschied, ob nur ein einzelner Name wie in diesem Fall abgefangen werden kann oder ob der Zugriff auf eine vollständige Liste aller Benutzernamen erfolgen kann. Letzteres birgt ein deutlich höheres Risiko, weil es ein besserer Ansatzpunkt für das Eindringen in ein System ist.

Der KAS bildet eine Antwort, die aus zwei Elementen besteht. Das erste ist ein Ticket, mit dem der Zugriff auf den TGS gewährt wird. Es wird auch als Ticket Granting Ticket (TGT) bezeichnet. Das zweite Element ist eine Zufallszahl, der TGS Session Key. Tickets sind eines der grundlegenden Konzepte von Kerberos. Ein Ticket enthält Informationen, die die Identität des Besitzers bestätigen und Zugriff zu Diensten gewähren. Tickets haben einen Gültigkeitszeitraum, der normalerweise mehrere Stunden umfasst. Nach Ablauf eines Tickets muss ein neues Ticket angefordert werden.

Die Nachricht - das verschlüsselte und nur dem KDC bekannte Ticket und der TGS Session Key - wird nun mit dem Kennwort des Benutzers, das dem KAS bekannt ist, verschlüsselt. Es wird dann zurück an den Benutzer gesendet. Der Client gibt nun sein Kennwort ein und verschlüsselt dieses ebenfalls. Das im Klartext eingegebene Kennwort wird gelöscht, während das verschlüsselte Kennwort wie auch später das TGT im Cache gehalten werden. Mit dem so verschlüsselten Kennwort kann nun die vom KDS erhaltene Nachricht entschlüsselt werden, so dass der Client sowohl über TGT als auch TGS Session Key verfügt.

Wenn nun der Zugriff auf einen Dienst im Netzwerk - also zum Beispiel einen File-Server oder einen Anwendungsserver - erfolgen soll, wird das TGT verwendet. War bisher alles noch ganz einfach, so wird es nun um einiges komplizierter.

Der Client formt aus . . .

- verschlüsseltem Ticket (TGT)
- verschlüsselter Authentisierung (Anmeldename, Netzadresse der Workstation, aktuelle Zeit)
- Name des Dienstes

eine Nachricht an den TGS. Die Authentisierung ist dabei mit dem TGS Session Key verschlüsselt. Die ersten beiden Elemente der Nachricht sind verschlüsselt, während das letzte Element ein Name ist und daher nicht verschlüsselt werden muss.

Der TGS erhält diese Nachricht und entschlüsselt zunächst das TGT. Aus diesem erhält er den TGS Session Key. Diesen kann er nun wiederum verwenden, um die Authentisierung zu entschlüsseln. Während also im ersten Fall - bei der Erlangung des TGT - das beiden Seiten bekannte Kennwort für die Verschlüsselung verwendet wurde, wird dieses Mal der beiden Seiten bekannte TGS Session Key eingesetzt.

Auf Basis der nun vorliegenden Informationen kann der TGS einige Integritätsüberprüfungen vornehmen:

?? Der Anmeldename im Ticket und in der Authentisierung müssen übereinstimmen.
?? Der Server; für den ein Ticket angefordert wird, muss existieren (beziehungsweise Kerberos bekannt sein).
?? Die Netzwerkadresse in der Authentisierung und in der enthaltenen Nachricht müssen übereinstimmen.

Wenn diese Bedingungen zutreffen, holt der TOS den Schlüssel für den angeforderten Dienst aus der Kerberos-Datenbank. Er erzeugt einen neuen Session Key und ein verschlüsseltes Ticket für den Dienst. Diese Information wird mit dem TGS Session Key, den die Workstation kennt, verschlüsselt und an diese gesendet.
Die Workstation kann die Nachricht entschlüsseln und erhält so ein verschlüsseltes Ticket für den Zugriff auf den Dienst. Sie erstellt - weil ja etwas Zeit verstrichen ist - eine neue Authentisierung, verschlüsselt diese mit dem neuen Session Key und sendet diese zusammen mit dem verschlüsselten Ticket und dem Namen des Servers an diesen.

Der Server kann nun mit dem ihm und Kerberos bekannten Schlüssel zunächst das verschlüsselte Ticket entschlüsseln. In diesem ist der neue Session Key enthalten, der wiederum verwendet werden kann, um die Authentisierung zu entschlüsseln. Und schon kann auf diesen Server zugegriffen werden, wenn mit der Authentisierung alles in Ordnung ist,

Das Update und die Ressourcen Domänen

Eine Ressourcen-Domäne unter NT wurde erstellt, um Server, Workstation, Accounts und Ressourcen logisch zu gruppieren und die zunächst nur einstufige Hierarchie von NT Domänen zu erweitern. Resourcen Domänen wurden eigentlich aus zwei Gründen erstellt:

?? Limitierung der Größe der SAM auf 40 MB
?? Delegationsmöglichkeit von administrativen Tätigkeiten an andere Domänen

Bei einem Update auf Windows 2000 existieren aufgrund der Struktur des Active Directory eine Reihe von Integrationsmöglichkeiten der alten NT Domänen in das Active Directory:

?? Upgrade der Domäne im gleichen Forest mit Hilfe der Delegationsmöglichkeiten von Windows 2000
?? Upgrade der Domäne in einen neuen Forest
?? Restrukturierung der Domäne in eine OU (Organizational Unit)

Welche Art des Updates Sie durchführen, hängt von der Organisationsstruktur und den zukünftigen Anforderungen an Ihre Verzeichnisdienste ab.

Upgrade und Administration

Nach einem Update von Windows NT wird die Domäne im sogenannten Mixed Mode geführt, um auch Downlevel Clients und Domänen Abwärtskompatibilität zu bieten. Nur im sogenannten Native Mode stehen alle neuen Verwaltungswerkezuge und die Replikationsmechanismen des AD und weitere Techniken zur Verfügung.

Mixed Mode

Im Mixed Mode agiert ein Windows 2000 Domain-Controller zusätzlich noch als PDC für NT BDCs. Standardmäßig agiert der erste Domänencontroller in einer Win2K Domain als PDC Emulator.

Es kann nur einen PDC Emulator pro Domäne existieren. Der PDC Emulator ist für folgende wichtigen Aufgaben zuständig:

- Emulation eines PDC und Replikation der SAM zu den BDC
- Durchführung von Account- und Paßwortänderungen
- Arbeit als Master Browser für NT Clients
- Zur Verfügungstellung von NT LAN Manager (NTLM) Authentifizierungs-Diensten
- Unterstützung von Active Diretory (AD) Replikation zu Win2K Domänen-Controllern und NTLM Replikation zu BDCs

In einer Win2K Site sollten Sie sicherstellen, dass Sie mindestens einen Win2K Domänen-Controller im Netzwerk haben, da Win2K Clients zuerst versuchen, eine Verbindung zu einem Win2K Controller mit DNS aufzunehmen. Wenn der Win2K Client keinen Win2K Domänen-Controller findet, versucht er per NTLM mit einem alten NT Domänen-Controller zu kommunizieren. NT unterstützt jedoch keine Group-Policies, so dass der Win2K Client nicht von den Vorteilen der Group-Policies über die Anmeldeskripte partizipieren kann.

Im Mixed Mode können NT Clients Ihre Passwörter nicht ändern, wenn der PDC Emulator, der Operation Master, nicht zur Verfügung steht.

Ein anderer Operation-Master, welcher im Netzwerk zur Verfügung stehen muss, ist der RID Operations Master. Der RID Operations Master stellt den NT Clients die SIDs zur Verfügung.

Ein weiterer Punkt, welcher Beachtung finden muss, ist die NT LAN-Manager Replikation (LMREPL) versus Win2Ks File Replication Service.

Native Mode

Der Native Mode unterstützt keine NT Domänen-Controller, es werden lediglich Win2K Maschinen unterstützt. Der Native Mode unterstützt die Universellen Gruppen, und die Sicherheitsgruppen, sowie die transitiven Vertrauensstellungen. Der größte aller Vorteile ist aber die unterstützt Skalierbarkeit des AD mit Millionen von Objekten.

Im Native Mode unterstützt das AD nur eine Größe von maximal 40 MB, weil aufgrund der Abwärtskompatibilität mit Windows NT die Replikation der Benutzer- und Gruppeninformationen auf 40 MB limitiert ist (Limit 40 MB der SAM).

Win2K erstellt automatisch Zwei-Weg Kerberos-Trusts mit den anderen Domänen in der Domäne. Da Windows NT DCs keine transitiven Trusts unterstützen, müssen die Vertrauensstellungen explizit festgelegt werden.

Im Native Mode werden die Gruppen-Richtlinien auch voll für alle Win2K Clients unterstützt. Wenn Sie in Ihrem Netzwerk die Systemrichtlinien und die Gruppenrichtlinien parallel laufen lassen, überschreiben die Systemrichtlinien die in den Gruppenrichtlinien festgelegten Einstellungen bei Redundanz. Es ist deshalb eine weitsichtige und geschachtelte Konfiguration notwendig.

Windows 2000 Gruppen

Windows 2000 unterstützt vier Typen von Sicherheits-Gruppen:

?? Lokale Gruppen
?? Domain Lokal Gruppen
?? Globale Gruppen
?? Universelle Gruppen

Lokale Gruppen

Lokale Gruppen existieren bereits unter Windows NT. Lokale Gruppen können als Mitglieder alle Mitglieder innerhalb des Forests enthalten, und auch Mitglieder von vertrauten Forests. In Bezug auf Ressourcen-Berechtigungen liegt ihr Einsatzbereich im Computer. Eine besondere Bedeutung haben die lokalen Gruppen auf dem PDC, da sie dort auf alle BDC repliziert werden und somit auch auf diesen einen Wirkungsbereich haben. Im Mixed Mode haben die lokalen Gruppen die gleiche Bedeutung wie unter NT.

Domain Lokal Gruppen

Domain Lokal Gruppen sind neu unter Windows 2000. Diese Gruppen sind nur verfügbar, wenn die Domäne im nativen Modus operiert. Domain Lokal Gruppen können als Mitglieder alle Mitglieder innerhalb des Forests enthalten, und auch Mitglieder von vertrauten Forests. Domain Lokal Gruppen haben ihren Wirkungsbereich innerhalb der Domäne.

Globale Gruppen

Globale Gruppen haben die gleiche Bedeutung wie die globalen Gruppen unter Windows NT und dienen der Berechtigungsvergabe über Domänengrenzen hinweg.

Universelle Gruppen

Universelle Gruppen gelten Forest-weit. Sie können Mitglieder von Windows 2000 Domänen im Forest enthalten. Universelle Gruppen sind jedoch nur im Native Modus verfügbar.

Universelle Gruppen haben eine besondere Bedeutung. Sie können Universelle Gruppen zum Beispiel dazu benutzen, sogenannte virtuelle Teams zu bilden. Diese Gruppen können weltweit, forest-weit oder auch nur lokal Bedeutung haben. Ein weiterer wichtiger Faktor bei der Verwendung von universellen Gruppen ist, dass die Mitglieder dieser im Global Catalog angezeigt werden, wohingegen Mitglieder von Domain Lokal Gruppen und Globalen Gruppen nicht im Global Catalog angezeigt werden.

Universelle Gruppen und Access Tokens

Wenn ein Benutzer Mitglied in einer universellen Gruppe ist, ist die SID dieser Gruppe im Access Token auf der Arbeitsstation enthalten und wird der Authentifzierung des TGT im KDC hinzugefügt.

ACHTUNG:

Es wird nicht empfohlen, Gruppen mit mehr als 5000 Mitgliedern zu erstellen.

Auswirkungen des Updates auf die Gruppen

Das Update von NT auf Windows 2000 hat keine Auswirkungen auf die Gruppen. Windows NT Local Groups werden zu Windows 2000 Local Groups und Windows NT Global Groups werden zu Windows 2000 Global Groups. Die wirkliche Änderung erfolgt beim Umswitchen in den Native Mode, bei dem die Lokalen Gruppen zu Domain Local Groups werden.

NetBIOS und WINS in Windows 2000

In einer reinen Windows 2000 Umgebung wird NetBIOS nicht mehr benötigt. Aus Abwärtskompatibilitätsgründen wird NetBIOS aber weiterhin Verwendung finden, bis alle Applikationen und Dienste auf WINS bzw. NetBIOS verzichten können und komplett auf DNS geschaltet werden kann.

Verfügbarkeit von LMRepl (LAN Manager Replication Service)

Windows NT Server bietet mit dem Verzeichnisreplikationsdienst eine Möglichkeit an, konsistente Datenbestände auf mehreren Servern zu pflegen. Von einem Export-Server werden Daten auf Importserver (auch NT Workstation) kopiert und so ein konsistenter Zustand erreicht. Einsatzgebiet der Verzeichnisreplikation sind die Anmeldeskripte, Systemrichtlinien und evtl. noch Default-Benutzerprofile.

Windows 2000 bietet den FRS (File Replication Service) als Alternative.

LMRepl wird nicht im Native und auch nicht im Mixed Modus unterstützt.

FRS wird automatisch installiert und erstellt auf jedem DC auf dem Systemdatenträger ein Verzeichnis namens SYSVOL, welches die Replikationen des AD (Multi-Master-Replikation), die Loginskripte usw. enthält. FRS kann lediglich auf DCs verwendet werden.

Um eine Brücke vom LMRepl zum FRS zu schaffen, können Sie einen Windows 2000 DC, welcher FRS unterstützt, so einstellen, dass er die Daten zu einem Windows NT repliziert, der LMRepl unterstützt.

RAS in einer Mixed-Mode Umgebung

Bei einer RAS Anmeldung unter NT wird meist der lokale System Account verwendet. Der lokale System Account loggt sich als sogenannte NULL-Session an, also ohne Name und Paßwort. Standardmäßig unterstützt Windows 2000 keine NULL-Sessions, nur NTLM und Kerberos, so dass RAS-Benutzer sich erst einmal nicht einwählen können, es sei denn . . .

?? Die Domäne ist im Mixed Mode und der Windows NT RAS Server ist ebenfalls ein BDC.
?? Die Domain ist in Mixed Mode und der Windows NT RAS Server ist ein BDC.
?? Die Domain ist in Mixed Mode oder Native Mode und die Active Directory Sicherheit wurde vernachlässigt, damit das Objekt JEDER lesenden Zugriff auf alle Objekte bekommt. Das Programm DCPROMO erlaubt diese Art der „laschen“ Sicherheitsvergabe.

Unterstützte Update-Pfade

Plattform	Update zu Windows 2000 Professional	Update zu Windows 2000 Server
Windows 3.x	Nein	Nein
Windows NT 3.1	Nein	Nein
Windows NT 3.1 Advanced Server	Nein	Nein
Windows NT 3.51 Workstation	Ja	Nein
Windows NT 3.51 Server	Nein	Ja
Windows 9x	Ja	Nein
Windows NT 4.0 Workstation	Ja	Nein
Windows NT 4.0 Server	Nein	Ja

Domain Restrukturierung

Die Frage nach dem Sinn oder Unsinn einer Domain-Restrukturierung kann nicht in einem Satz beantwortet werden und hängt ganz von vielen Faktoren der jeweiligen Organisationen ab.

Grundsätzlich lassen sich drei zeitliche Unterscheidungen bei der Domänen-Restrukturierung aufzeigen:

?? Post-Upgrade
?? On-The-Fly Upgrades
?? Post-Migration

Bei der Post-Migration wird die vorhandene NT Domänenstruktur schon vorher restrukturiert und auf die künftigen Anforderungen und auf die Besonderheiten des Active Directories angepasst.
Bei der On-The-Fly Migration wird während des Upgrades auf Win2K auch die Resturkturierung der Domänen durchgeführt.

Bei der Post-Migration wird die Win2K nach erfolgtem Upgrade restrukturiert.

Warum soll überhaupt restrukturiert werden

?? Höhere Skalierbarkeit

Die 40 MB Grenze der SAM von Windows NT wird mit Windows 2000 aufgehoben. Windows 2000 unterstützt, im Gegensatz zu Windows NT, zusätzlich noch das Multi-Master Replikationsmodell. Somit hat jeder DC im AD eine Read-Write Kopie der Datenbank. Dadurch wird eine größere Skalierbarkeit erreicht. Das AD kann theoretisch Millionen von Objekten speichern. Die Größe des AD ist auf 17 TB begrenzt.

?? Feinere Granularität bei der Delegation von administrativen Aufgaben

Mit Hilfe der Strukturierungsmöglichkeit der Domänen im AD in OU=organisatorische Einheiten, ist eine feinere Granulation und Delegation der Berechtigungen für einzelne Domänen, organisatorische Einheiten usw. möglich. Außerdem können Berechtigungen jetzt noch differenzierter als unter Windows NT vergeben werden.

?? Einfachere Administration

Durch die automatischen transitiven Vertrauensstellungen braucht der Administrator die komplizierten Vertrauensstellungen aus NT 4.0 nicht mehr zu konfigurieren. Die Delegation von administrativen Berechtigungen erlaubt die Verteilung von administrativen Aufgaben auf organisatorischer und auch funktionaler Ebene.

SIDhistory

Um die Restrukturierung und die Verschiebung von Ressourcen innerhalb des Active Directories zu erleichtern, ohne den Bezug zu der SID zu verlieren, existiert

die sogenannte SIDhistory. Die SIDhistory ist ein Attribut des Active Directory Security Prinzipals und wird dazu benutzt, die ehemalige SID zu speichern und einen Zeiger auf das oder die verschobenen Objekte zu legen, welche jetzt eine neue SID besitzen.

Mit dem Programm MOVETREE.EXE von Windows 2000 können Objekte im Active Directory verschoben werden. Das Programm MOVETREE.EXE verwendet auch die SIDhistory.

MOVETREE.EXE benötigt jedoch folgende Zustände:

- Mixed-Mode oder Native –Mode Domain
- Native Mode Target Domain
- Source und Target Domain im selben Forest
- Leere Globale Gruppen

Verschieben eines Servers

Das Verschieben eines Servers in eine andere Domäne bereitet keine Probleme, weil hier ebenfalls die SIDhistory angewendet wird. Referendierende ACLs zu der lokalen Gruppe der Maschinen-Accounts existieren in der lokalen SAM-Datenbank des Rechners und unterliegen somit nicht der SID-Änderung.

Windows NT 3.51 und die SIDhistory

Bei der Planung der Migration von NT 3.51 auf Windows 2000 sind einige Besonderheiten zu beachten. Das Problem existiert bei der Authentifizierung und Authorisation der Access Tokens bei Windows NT 3.51. Wenn ein Benutzer interaktiv oder Remote über das Netzwerk authentifiziert wird, wird das Token nur aus der relativen SID zu der User-Account Domain gebildet (also aus den Gruppen der Server und Workstations, von denen die Authentifikation erfolgte). Das Resultat ist, dass Windows NT 3.51 Access Tokens keine Universellen Gruppen als Mitglied von anderen Domänen haben können. SIDs von anderen Domänen werden also unter NT 3.51 ignoriert, was in einer Vielzahl der Fällen zu einem „ZUGRIFF VERWEIGERT“ führen wird.

Profiles und die SIDhistory

Bei der Anmeldung eines Benutzers wird ein Benutzerprofil, welches mit der SID des Benutzers verbunden ist, geladen. Das Benutzerprofil befindet sich bei einem lokalen Benutzerprofil auf der Festplatte der Workstation. Das System ermittelt den Speicherort des Benutzerprofils anhand der Einträge in der Registry unter HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList.

Nach erfolgter Migration kann es sein, dass das Benutzerprofil für den Benutzer verloren geht, da nach der Migration sich die referenzierende SID der Domäne geändert hat, aber auf der Workstation für das Benutzerprofil immer noch die alte SID gespeichert ist.

Wenn der Benutzer zwischen Windows 2000 Domänen innerhalb des gleichen Forests mit Hilfe des Tools MOVETREE verschoben wird, ist das kein Problem, weil MOVETREE.EXE die GUID des Benutzers bewahrt. Wenn es dann bei der Verwendung des Profiles Probleme gibt, kann anhand der GUID festgestellt werden, wo sich das Profile befindet. Unter HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileGID, befindet sich ein Schlüssel mit einem String des Users GID.

Profile Migration

Bei der Profile-Migration stehen zwei verschiedene Möglichkeiten zur Verfügung:

Gemeinsam genutzte Profile

Bei dieser Art werden die Benutzerprofile von einer gewissen Anzahl Benutzer gemeinsam genutzt. Eine Kopie des Benutzerprofils kann von mehreren Benutzern genutzt werden.

Kopierte Profile

Bei dieser Art der Benutzerprofile wird das Benutzerprofil eines Benutzers von seiner Original-Lokation an eine andere Stelle für die Verwendung durch einen anderen Benutzer kopiert. Jeder Benutzer-Account hat so sein eigenes Benutzerprofil. Änderungen des Benutzers werden für jedes Benutzerprofil einzeln vorgenommen.

Cloning Security Principal

Cloning Security Principals erlaubt das sogenannte Cloning von NT 4 Benutzer- und Gruppen-Accounts in Windows 2000 ohne diese aus der NT 4 Domäne zu entfernen.

Beim Cloning werden auch die assoziierten SIDs der Accounts mit geclont.
Mit Hilfe von VB können Scripts erstellt werden, die das Cloning automatisieren.

Cloning Security Principals setzt folgende Zustände voraus:

- Die Source und Target Domäne dürfen nicht im gleichen Forest sein
- Die SID des Source Accounts muss in der Target-Domäne als primäre SID oder in der SIDhistory existieren
- Um das Programm ClonePrincipal ausführen zu dürfen, werden Domänen-Administratorrechte benötigt.
- Die Sicherheitsüberwachung sollte auf der Target-Domäne eingeschaltet werden