

## WINDOWS 2000 Active-Directory

Microsoft verspricht mit WINDOWS 2000 einen vollständig überarbeiteten und skalierbaren Verzeichnisdienst. Dieser bietet dem Administrator zahlreiche neue Features, verlangt aber zugleich sorgfältige Planung bei der Einführung. Wer heute eine NT-4.0-Domäne plant, sollte dies gleich im Hinblick auf eine spätere Migration auf WINDOWS 2000 tun. Network Computing zeigt, was zu beachten ist.

### VON DIRK PELZER

#### Was ist ein Verzeichnisdienst

Ein Verzeichnisdienst (Directory-Service) kann allgemein als Speicher bezeichnet werden, der in der Lage ist, Informationen über bestimmte Bereiche, oder abstrakter ausgedrückt Objekte abzulegen und zu verwalten. Ein beliebtes Beispiel in diesem Zusammenhang ist der Vergleich mit einem Telefonbuch. Dieses enthält zum Beispiel Angaben über Personen, Telefonnummern, sowie möglicherweise Faxnummern, Adressen und so weiter. Im Netzwerkbereich enthält ein Verzeichnisdienst für den Netzwerkbetrieb relevante Informationen, wie zum Beispiel Angaben über Benutzernamen, Email-Adressen, Netzwerkanwendungen, Konfigurationsdaten für Desktop-Applikationen und vieles mehr. Während die genannten Informationen in der Regel auch ohne Verzeichnisdienst vorhanden sind, wäre die bloße Zusammenfassung in einem Verzeichnisdienst noch nichts Besonderes. Der Vorteil des Directory-Service ist, daß Administratoren, Endanwender und Anwendungen über den Verzeichnisdienst nach Informationen suchen können. Analog einem elektronischen Telefonbuch, in dem der Benutzer anhand einer Telefonnummer einen Namen ermitteln kann, kann ein Anwender im Netzwerkbereich zum Beispiel alle Server suchen und anzeigen lassen, die eine bestimmte Funktion, sei es eine Anwendung oder einen Dienst, zur Verfügung stellen. Ein weiterer Vorteil eines Verzeichnisdienstes ist, daß der Administrator sein Netzwerk hierarchisch strukturieren kann und gleichzeitig ein Werkzeug erhält, um das gesamte Directory zentral zu verwalten.

Active-Directory (AD), das mit der Einführung von WINDOWS 2000 verfügbar sein wird, ist ein solcher Verzeichnisdienst, der zusätzlich noch über einige weitere Eigenschaften verfügt. So kann der Administrator alle Objekte des Active-Directory über

eine Zugriffsliste (Access-Control-List) sichern und so die Integrität der Daten gewährleisten und den Zugriff durch Unbefugte wirksam unterbinden. Die im Active-Directory gespeicherten Objekte sind aber nicht nur zentral über einen einzelnen Server zu verwalten und abzufragen, sondern lassen sich verteilen und replizieren. Dazu verwendet WINDOWS 2000 das Konzept der Domain-Controller. Das gibt es zwar im Prinzip auch schon bei den bisherigen NT-Versionen, jedoch entfällt bei WINDOWS 2000 der Unterschied zwischen Primary- und Backup-Domain-Controller. Hier sind alle Domain-Controller gleichberechtigte Partner, die über dieselben Informationen verfügen und auf diese auch schreibend zugreifen können. Ein Replikationsmechanismus sorgt dafür, daß die Inhalte der Active-Directory-Datenbank ständig auf allen Domänen-Controllern aktuell sind. Microsoft spricht in diesem Zusammenhang von »Multi-Master-Replication«. Die im Active-Directory enthaltenen Objekte sind im Gegensatz zu dem Verzeichnisdienst der aktuellen NT-Version nicht statisch, sondern nahezu beliebig erweiterbar. So kann der Administrator bestehende Objekte um zusätzliche Attribute erweitern oder aber sogar völlig neue Objekte hinzufügen. Das sollte jedoch mit Bedacht geschehen, da sich einmal hinzugefügte Objekte und Attribute nicht mehr ohne weiteres entfernen lassen. Active-Directory wurde in Anlehnung an den X.500-Standard der ITU entwickelt, stellt aber keine X.500-Implementierung dar. So unterstützt AD zwar das Lightweight-Directory-Access-Protokoll (LDAP) in der Version 2 und 3, jedoch nicht andere vom X.500-Standard geforderte Protokolle, wie das Directory-Access-Protokoll oder das Directory-System-Protokoll. Dafür hat Active-Directory das Schema gemäß X.520/X.521 implementiert und trägt damit der Forderung der von LDAP geforderten Attribute Rechnung.

#### Aufbau des Active-Directory

Eines der Grundelemente des Active-Directory

ist, ähnlich wie bei den bisherigen NT-Versionen bis einschließlich der Version 4.0, die Domain (Domäne). Das Active-Directory besteht aus mindestens einer solchen Domäne, kann aber auch mehrere gleichzeitig umfassen. Es ist in diesem Zusammenhang auch wichtig zu erwähnen, daß der Namensraum des Active-Directory eng verzahnt ist mit dem Domain-Name-System (DNS), dem Standard-Namensdienst des Internet. Der Name einer Active-Directory-Domain muß den Konventionen von DNS genügen. So ist zum Beispiel abc.com unter WINDOWS 2000 sowohl ein DNS-Name, als auch eine Active-Directory-Domain. Domains lassen sich durch »Organizational-Units« (OUs) weiter untergliedern. Das ermöglicht es dem Administrator, die Struktur eines Unternehmens auf der Netzwerkebene nachzubilden. So kann er zum Beispiel einer Domäne abc.com die OUs Entwicklung, Personalwesen, Buchhaltung und gegebenenfalls weitere hinzufügen. Organizational-Units können auch rekursiv sein, das heißt unterhalb einer OU können, ähnlich wie bei einem Dateisystem, weitere OUs hinzugefügt werden. In jede OU kann der Administrator die Objekte einbinden, die logisch dorthin gehören, wie zum Beispiel Benutzer oder Sicherheitsrichtlinien. Zusätzlich erlaubt AD dem Netzwerkverwalter einzelnen Anwendern ausgewählte administrative Rechte für einen bestimmten Bereich, also zum Beispiel eine Organizational-Unit, zu vergeben. So kann einem Projektleiter das Recht übertragen werden, eine eigene OU zu Testzwecken vollständig oder teilweise selbst zu verwalten, also beispielsweise Benutzer hinzuzufügen und zu entfernen, oder Drucker zu verwalten. Diese Rechte gelten dann jedoch nur für diese spezielle Organizational-Unit und nicht für andere OUs oder gar die gesamte Domäne. Das stellt einen wesentlichen Fortschritt gegenüber dem bisherigen Domänenkonzept der NT-Versionen bis einschließlich 4.0 dar. Hier müßte man, um dasselbe zu erreichen eine neue Domäne einrichten.

Jede Domain hat ihre eigenen Sicherheitsrichtlinien und Beziehungen zu anderen Domains. Werden mehrere Domains über Vertrauensbeziehungen miteinander verknüpft und wenn sie über ein gemeinsames Schema verfügen, so bezeichnet man dies als »Domain-Tree«. Mehrere Domain-

Trees wiederum können in einem »Forest« zusammengefaßt werden. Die Vertrauensbeziehungen zwischen den Domänen werden dabei über das Kerberos-Sicherheitsprotokoll abgewickelt. Es ist zu beachten, daß solche Kerberos-Vertrauensstellungen standardmäßig transitiv sind. Das heißt also in einem Beispiel mit drei Domänen A, B und C, wobei A der Domäne B vertraut, und B der Domäne C, daß automatisch Domäne A auch Domäne C vertraut. Dadurch reduziert sich speziell in komplexeren Umgebungen die Zahl der zu verwaltenden Vertrauensbeziehungen erheblich.

Ein letzter Begriff, der im Zusammenhang mit Active-Directory genannt werden muß, ist die Site. Eine Site beinhaltet einen oder mehrere Active-Directory-Server, die sich entweder im selben oder unterschiedlichen IP-Subnetzen befinden. Die Verknüpfung zwischen Sites und Subnetzen ermöglicht es dem Administrator, Einfluß auf das Netzwerkverhalten des Active-Directory zu nehmen und speziell den Verkehr, der durch den Replikationsmechanismus entsteht besser zu steuern. Zusätzlich wird es für Active-Directory-Clients einfacher einen Anmelde-Server zu finden, der sich netzwerkseitig betrachtet in ihrer unmittelbaren Umgebung befindet. Der Client sucht nämlich bei der Anmeldung eines Benutzers nach einem Domain-Controller, der sich in derselben Site befindet, wie er selbst. Für die Planung eines AD-Konzeptes ist es wichtig, den Unterschied zwischen Site und Domäne verstanden zu haben und beide Aspekte getrennt voneinander zu betrachten. Während sich die Site auf die physikalischen Gegebenheiten des Netzes bezieht, dient die Domäne dazu, die Unternehmensstruktur logisch auf das NT-Netz abzubilden und ist somit zunächst unabhängig von der zugrundeliegenden Physik.

#### Planung eines Active-Directory-Konzeptes

Bei der Planung eines AD-Konzeptes gibt es eine Menge an Parametern, die zu beachten sind, will man ein optimales Ergebnis bezüglich Verfügbarkeit, Performance und Kosten erreichen. Folgende Faustregeln sollen die Entscheidung erleichtern.

- Wenn alle Rechner eines Netzes über eine schnelle LAN-Verbindung miteinander kommunizieren, macht es Sinn, nur eine Site zu konfigurieren.
- Ist das Netzwerk durch langsame WAN-Verbindungen getrennt, so kann es sinnvoll sein, für jeden entfernten Standort eine eigene Site einzurichten. Das hängt wiederum davon ab, ob es notwendig ist, einen Domain-Controller in den entfernten Standorten aufzustellen. Ist aufgrund einer geringen Anzahl von Clients kein DC erforderlich, entfällt natürlich auch der Replikationsverkehr und somit die Notwendigkeit, eine separate Site zu konfigurieren.
- Das Active-Directory sollte am besten nur aus einer einzigen Domäne und den dazugehörigen Organizational-Units bestehen. Das erleichtert die Administration und schafft Übersicht. Da das Active-Directory mehr als zehn Millionen Objekte mit einer Datenbankgröße von 17 Terabyte aufnehmen kann, sind so schnell keine Engpässe zu befürchten.
- Der Aufbau eines Domain-Trees oder gar eines Forest sollte nur in Betracht gezogen werden, wenn es aus verwaltungstechnischen oder geschäftlichen Erwägungen heraus sinnvoll und notwendig ist. Das kann beispielsweise bei großen internationalen Konzernen der Fall sein, die über eine dezentrale Administration an mehreren Standorten verfügen. Die Bildung von Forests bieten sich bei der Fusion von Firmen oder der Aufteilung eines Unternehmens in verschiedene weitgehend voneinander unabhängige Sparten an.
- Ist die Verbindung zwischen zwei Abschnitten eines Netzwerks so langsam, daß eine Replikation von AD-Informationen unerwünscht ist, sollten unterschiedliche Domänen definiert werden, um den Replikationsverkehr zu verhindern. Falls es möglich ist, die Replikation nur zu bestimmten Zeiten durchführen zu lassen, weil dann kein oder nur wenig anderer Netzwerkverkehr herrscht, bietet sich alternativ die Einrichtung einer Domäne mit zwei getrennten Sites an.
- Besteht in einer Netzwerkumgebung eine Notwendigkeit, für einheitliche Sicherheitsrichtlinien, so sollte das Active-Directory auf jeden Fall aus einer einzelnen Domäne bestehen. Da jede Domäne über eigene Sicherheitsrichtlinien verfügt, müßte beim Einsatz mehrerer Domänen jede

einzelne mit den jeweiligen Sicherheitsrichtlinien konfiguriert werden, was in der Praxis nicht immer zu 100 Prozent möglich sein dürfte.

#### Planung einer NT 4.0-Domäne im Hinblick auf eine Migration auf WINDOWS 2000

Wer heute vor der Entscheidung steht, ein Domänen-Konzept für NT 4.0 zu machen, sollte dies bereits im Hinblick auf eine spätere Migration auf WINDOWS 2000 tun. Hierbei gibt es einige Dinge zu beachten. Das beginnt bereits auf der Ebene der Transport- und Routingprotokolle. So setzt Active-Directory voraus, daß ein TCP/IP-Netz mit DNS zur Namensauflösung vorhanden ist. Es werden zwar nach wie vor andere Protokolle, wie IPX oder NetBEUI unterstützt, jedoch nur in Verbindung mit sogenannten Downlevel-Servern und Clients, wie zum Beispiel Windows-für-Workgroups 3.11 oder Windows-NT 4.0. Auch ein WINS-Server zur Auflösung von NetBIOS-Namen wird in WINDOWS 2000 enthalten sein, jedoch ebenfalls nur aus Kompatibilitätsgründen mit früheren Windows-Versionen. WINDOWS 2000 wird darüber hinaus dynamisches DNS unterstützen. Dies bedeutet für den Administrator eine erhebliche Arbeitserleichterung, da er hiermit die Möglichkeit erhält, daß Clients ihre IP-Adressen selbst beim DNS-Server registrieren und nicht mehr manuell in die DNS-Zonen-Dateien eingetragen werden müssen. Insbesondere in Verbindung mit dem Dynamic-Host-Configuration-Protokoll (DHCP) wird der Einsatz von dynamischem DNS noch interessanter, da sich der Administrator hierbei nicht einmal mehr darum kümmern muß, welcher Client welche IP-Adresse erhält. Wer also heute eine NT 4.0-Domäne plant sollte bereits jetzt TCP/IP als Standardprotokoll verwenden und DNS zur Namensauflösung einsetzen (Siehe DNS-Workshop in Network Computing x/98). Da unter NT 4.0 der DNS-Server auch auf Daten des WINS-Servers zugreifen kann, ist es nicht unbedingt erforderlich, alle Maschinen manuell in die DNS-Zone-Files einzutragen. Statt dessen sollte der Administrator die Integrationsfähigkeit von DNS und WINS nutzen. Empfehlenswert ist auch der Einsatz von DHCP um die Clients automatisch mit den notwendigen IP-Parametern,

wie IP-Adresse, Subnetzmaske, DNS-Domain, etc. zu versorgen. Bei der Namensgebung von Clients und Servern sollte darauf geachtet werden, daß diese den Regeln von DNS entspricht. Gültige DNS-Namen dürfen folgende Zeichen enthalten: »a-z«, »A-Z«, »0-9« und das Minuszeichen.

Was die Domänenstruktur eines zu planenden NT 4.0-Netztes anbelangt, so ist anzuraten, diese möglichst einfach zu halten sein und im Idealfall nur aus einer einzigen Domäne aufzubauen. Dies wird bei vielen Firmen kleiner und mittlerer Größe ohnehin der Fall sein. Große Konzerne mit mehreren tausend Benutzern werden jedoch in der Regel um ein Modell, das mehrere Domänen umfaßt nicht umhin kommen. Doch auch hier gilt je einfacher das Modell unter NT 4.0, desto leichter wird später die Migration auf WINDOWS 2000 sein. Um die Migration zu vereinfachen, unterstützt die künftige NT-Version eine gemischte Umgebung aus WINDOWS-2000-Active-Directory-Domain-Controllern und NT-4.0-Domain-Controllern. Dabei präsentieren sich die WINDOWS-2000-Domain-Controller Downlevel-Clients wie Windows-für-Workgroups gegenüber wie NT-4.0-Domain-Controller.

Unter NT 4.0 kommt in der Regel eines von vier Domänenmodellen zu Einsatz:

- Single-Domain
- Master-Domain
- Multiple-Master-Domain
- Complete-Trust

Außer beim Single-Domain-Modell, basieren die übrigen Modell auf einem Konzept von Master-Domains und Resource-Domains. Dabei werden in den Master-Domains die Benutzerkonten verwaltet und in den Resource-Domains befinden sich die zur Benutzung freigegebenen Ressourcen, wie Datei- und Druckdienste. Die Migration eines Single-Domain-Modells gestaltet sich relativ einfach, da die NT-4.0-Domäne in der Regel in eine einzelne WINDOWS-2000-Domäne überführt wird. Die Migration erlaubt dem Administrator durch die Definition von Organizational-Units die Unternehmensstruktur besser auf der Netzwerkebene abzubilden und zusätzlich von den Möglichkeiten der

Delegierung administrativer Rechte Gebrauch zu machen.

Beim Master-Domain-Modell, in dem es eine Master-Domain und eine oder mehrere Resource-Domains gibt, hat Administrator zwei Möglichkeiten der Migration. Entweder er behält die bisherige Struktur bei, migriert jede Domäne und fügt die Domänen anschließend in einem Domain-Tree zusammen, oder er konsolidiert die Struktur und migriert die vorhandenen Domänen in eine einzige Domäne. Letzter Schritt macht vor allem dann Sinn, wenn das Unternehmen über eine zentralisierte EDV-Administration verfügt, bei der alle Aktivitäten von einer zentralen Stelle aus koordiniert werden. Davon unbenommen können natürlich mit dem Active-Directory OUs gebildet und administrative Rechte an Dritte delegiert werden. Die Migration zu einer einzelnen Domain hat aber noch weitere Vorteile. So müssen zum Beispiel keine Vertrauensstellungen mehr verwaltet werden. Durch den Verzicht auf mehrere Domänen wird zudem die Suche nach Informationen im Active-Directory beschleunigt.

Das Multiple-Master-Domain-Modell wird in der Regel von sehr großen Firmen eingesetzt, die über eine dezentrale Administration in mehreren Lokationen verfügen oder aber so viele Benutzer haben, daß sie nicht in einer einzelnen Domäne verwaltet werden können. Auch hier bietet sich die Möglichkeit, das bestehende Modell eins zu eins zu migrieren oder abhängig von den Gegebenheiten das Modell zu konsolidieren. Da bei der Migration des Multiple-Master-Domain-Modells sehr viele Aspekte, wie zum Beispiel LAN-/WAN-Verbindungen, administrative Zuständigkeiten, Unternehmensstruktur und weitere berücksichtigt werden müssen, ist für die Migration kein Patentrezept möglich. Je nach Gegebenheiten macht die Migration zu einer einzelnen Domäne, zu einem Domain-Tree oder einem Forest mehr oder weniger Sinn. Dasselbe gilt für das Complete-Trust-Modell.

Ist erst einmal festgelegt, wie ein bestehendes Modell zu migrieren ist, lassen sich allgemein einige Schritte für das weitere Vorgehen definieren. Zunächst einmal sollte auf dem Primary-Domain-

Controller (PDC) ein Update auf WINDOWS 2000 erfolgen. Unter Umständen kann es auch sinnvoll sein, einen zusätzlichen NT 4.0-Server zu installieren, diesen zum Primary-Domain-Controller zu machen und anschließend ein Update auf WINDOWS 2000 durchzuführen. Wer diesen Weg einschlägt kann sicher sein, daß an der Konfiguration der bestehenden Server zunächst nichts geändert wird und bei Problemen mit dem WINDOWS-2000-Server jederzeit einer der »alten« Backup-Domain-Controller zum Primary heraufgestuft werden kann.

Der Vorteil dieser Vorgehensweise besteht darin, daß die Domäne nun mit Active-Directory betrieben werden kann und sich gegebenenfalls in einen bereits bestehenden Domain-Tree einbinden läßt. Zum anderen werden neue Objekte, wie zum Beispiel Benutzer dann gleich im Active-Directory angelegt. Zusätzlich kann der Administrator bereits damit beginnen, OUs zu bilden und diesen Objekte zuzuordnen. Da der WINDOWS-2000-Domain-Controller zu diesem Zeitpunkt die AD-Objekte für Downlevel-Computer »übersetzt«, ist die Umstellung für sie vollkommen transparent. Auch die bestehenden Backup-Domain-Controller merken nichts, denn für sie agiert der WINDOWS-2000-Server wie ein NT-4.0-Primary-Domain-Controller. Clients, die schon Active-Directory verstehen, wie WINDOWS-2000-Workstation oder Windows 9x mit Active-Directory-Client-Software können die Fähigkeiten des Active-Directory-Server nutzen und mit dessen Möglichkeiten verwaltet werden. So können bereits zu diesem Zeitpunkt die ganzen Vorteile des Active-Directory für die neueren Clients genutzt und gleichzeitig die Downlevel-Clients ohne Funktionsverlust weiter betrieben werden.

Im nächsten Schritt sollte einer der NT-4.0-Backup-Domain-Controller auf WINDOWS 2000 umgestellt werden. Damit ist dann gewährleistet, daß die Active-Directory-Information beim Ausfall des PDC weiter zur Verfügung steht. Die übrigen NT-4.0-BDCs sollten noch eine Weile weiter bestehen bleiben, so daß im Fall, daß es zu Problemen mit dem Active-Directory oder dem WINDOWS-2000-Server kommt jederzeit ein Fallback auf einen der bestehenden NT-4.0-Server durchgeführt werden

kann. Sobald sich gezeigt hat, daß die neue Konfiguration zufriedenstellend läuft, ist es an der Zeit, nach und nach die verbliebenen NT-4.0-BDCs auf WINDOWS 2000 umzustellen. Ist das erfolgt, kann der Administrator die Migration der Domain abschließen und vom Mischbetrieb auf reinen Active-Directory-Betrieb umstellen. Das hat jedoch weitreichende Konsequenzen und sollte gut bedacht sein. Sobald die Umstellung vollzogen wurde gelten folgende Bedingungen:

- Der Primary-Domain-Controller unterstützt keine Replikation der Benutzerdatenbank nach NT-4.0-Standard mehr.
- Es können keine Downlevel-NT-Domain-Controller mehr in die Domäne hinzugefügt werden.
- Der WINDOWS-2000-Server der während der Migrationsphase als PDC fungiert hat, gibt diese Rolle auf und alle Domain-Controller agieren von diesem Zeitpunkt an als gleichberechtigte Partner.
- Die Domain nutzt das neue Active-Directory-Replication-Protokoll zum Abgleich der Active-Directory-Datenbanken der Domain-Controller untereinander.
- Downlevel-Clients können transitive Vertrauensstellungen innerhalb des Domain-Trees nutzen auch wenn sie noch nicht über Active-Directory-Client-Software verfügen. Die Domain-Controller sorgen dafür, daß die Clients sich in jeder Domain des Domain-Tree anmelden und die zur Verfügung stehenden Ressourcen nutzen können.
- Es gibt keine lokalen und globalen Benutzergruppen mehr. Active-Directory kennt nur noch eine Art von Gruppe, die jeden beliebigen Benutzer und jede beliebige Gruppe des Domains-Trees aufnehmen kann.

#### Fazit

Die Umstellung bestehender NT-4.0-Domänen sollte sorgfältig geplant und am besten erst einmal unter Laborbedingungen durchexerziert werden. Keinesfalls sollten Administratoren übereilt handeln und »mal eben schnell« ein Update ausprobieren. Dazu sind die Auswirkungen, die sich ergeben können viel zu gravierend.

## Wichtige Begriffe kurz erläutert

### Domain

Als Domain bezeichnet man eine Gruppe von Servern (Domain-Controller), die unter einem gemeinsamen Namen Objekte eines Netzwerks zusammenfassen und bezüglich der Sicherheitsrichtlinien eine Einheit darstellen. Der Administrator einer Domäne kann nur die Objekte der eigenen Domäne verwalten, nicht jedoch die anderer Domänen. Eine Domain kann durch Verwendung von Organizational-Units (OUs) in logische Einheiten aufgegliedert werden, die beispielsweise den verschiedenen Abteilungen eines Unternehmens entsprechen. Eine Domain kann maximal zehn Millionen Objekte, also Benutzer, OUs, Computer, etc. umfassen.

### Domain-Tree

Ein Domain-Tree ist eine hierarchische Anordnung von Domains über Vertrauensbeziehungen. Da diese Vertrauensbeziehungen standardmäßig transitiv sind und auf Gegenseitigkeit beruhen, hat automatisch jede Domain, die einem Domain-Tree hinzugefügt wird, eine Vertrauensbeziehung zu jeder anderen Domain innerhalb des Domain-Tree.

### Forest

Ein Forest ist eine Verknüpfung mehrerer Domain-Trees, wobei die einzelnen Domain-Trees keine gemeinsame Namensgebung aufweisen. So können zum Beispiel die Domains abc.com und xyz.com mit ihren jeweiligen Subdomains in einem Forest zusammengefügt werden und auf diese Weise ein gemeinsames Schema und einen gemeinsamen Global-Catalog erhalten.

### Site

Eine Site ist definiert als ein oder mehrere IP-Subnetze, wobei die darin befindlichen Rechner über Netzwerkverbindungen mit hoher Geschwindigkeit verknüpft sind. Durch die Einführung von Sites wird erreicht, daß die logische Struktur einer Domain nicht notwendigerweise der physikalischen Struktur entsprechen muß. Die physikalische Struktur wird einfach über Sites abgebildet, die dafür sorgen daß der Netzwerkverkehr zwischen

mehreren Sites einer Domain geringer ausfällt, als der innerhalb einer Site. Bereiche eines Netzes, die durch WAN-Verbindungen, mehrere Router oder andere langsame Verbindungen getrennt sind, sollten als separate Sites definiert werden.

### Organizational-Unit

Organizational-Units sind innerhalb einer Domain Behälter, in denen der Administrator Benutzer, Gruppen, Dateien oder andere OUs ablegen kann, um das Netzwerk besser strukturieren zu können. Durch den Einsatz von OUs ist es möglich, einen hierarchischen Namensraum zu schaffen, der dem tatsächlichen Aufbau einer Firma nachempfunden ist. OUs tragen aber auch dazu bei, administrative Aufgaben leichter an ausgewählte Anwender übertragen zu können. So können bestimmte Rechte, wie etwa das Anlegen eines neuen Benutzers oder das Löschen von Druckaufträgen an einzelne Benutzer einzelner OUs delegiert werden. Diese Benutzer können dann die ihnen zugewiesenen administrativen Aufgaben in der entsprechenden OU durchführen, haben jedoch in anderen OUs keine entsprechenden Privilegien. Active-Directory-OUs sind nicht äquivalent zu X.500-OUs. Die Namen von OUs finden keine Berücksichtigung im DNS-Namensraum.

### Global-Catalog

Der Global-Catalog ist ein Dienst, der Informationen von allen Domains eines Forest enthält und diese dem Anwender oder Applikationen zugänglich macht. Dabei können sämtliche Domains nach einer beliebigen Anzahl von Attributen durchsucht werden. Der Administrator entscheidet, welcher Domain-Controller zum Global-Catalog-Server ernannt wird.

### Schema

Das Schema ist die formale Definition aller Objekte, die in einem Verzeichnisdienst gespeichert werden können. NT 5 beinhaltet ein Schema, das die am häufigsten Objekte, wie Benutzer, Gruppen, Sicherheitsrichtlinien, Domains, und so weiter definiert.

### Domain-Controller

Jede NT-5-Domäne besteht aus mindestens einem Domain-Controller (DC), der die Active-Directory-

## WINDOWS 2000 Active-Directory

Datenbank verwaltet. Er ist zugleich Replikationspartner anderer DC einer Domain und sorgt dafür, daß das Active-Directory konsistent bleibt.

### Zur Person

DIPL. ING. DIRK PELZER arbeitet als freier Consultant und Journalist in München. Er betreibt ein Storage Labor für verschiedene namhafte Fachzeitschriften. Zudem beschäftigt er sich mit Speichernetzen und Hochverfügbarkeit.

