1. Grundlegende Netzwerkkonzepte

Vorteile der Vernetzung
- Gemeinsame Nutzung von Informationen
- Zentralisierung von Verwaltung und Support
- Gemeinsame Nutzung von Hardware und Software

Anmelden an ...
...einer Arbeitsgruppe:
Meldet sich ein Benutzer an einem Rechner einer Arbeitsgruppe an, so werden die Eingabedaten in der lokalen SAM des Rechners überprüft. Existiert das betreffende Konto, so wird das Benutzerprofil geladen, sonst erfolgt eine Fehlermeldung.

...einer Domäne:
1. Beim Anmelden an der Domäne werden die Anmeldedaten zum Active Directory des Domänencontrollers übertragen und dort erfolgt dann die Authentifizierung. Existiert ein entsprechendes Konto, so wird das Profil des Benutzers geladen und der Benutzer erhält gemäß seiner Berechtigungen Zugriff auf die Ressourcen der Domäne.
2. Lokale Anmeldung: Siehe Arbeitsgruppe. Der Benutzer hat bei erfolgreicher Anmeldung nur Zugriff gemäß seinen Berechtigungen auf die Ressource des lokalen Rechners.

Netzwerkbetriebssystem
- Ermöglicht dem Computer den Betrieb in einem Netzwerk
- Stellt für Computer in einem Netzwerk die Basisdienste bereit
    - Koordiniert die Aktivitäten der unterschiedlichen Geräte
    - Ermöglicht den Clientzugriff auf Netzwerkressourcen
    - Stellt die Sicherheit von Daten und Geräten sicher
- Unterstützt Mechanismen, mit denen Anwendungen in die Lage versetzt werden, miteinander zu kommunizieren
- Ist in anderen bekannten Betriebssystemen integriert

Wozu benötigt man das Betriebssystem Windows 2000 Server?
Computer werden aus diversen Gründen vernetzt. Dabei werden die Rechner zunächst physikalisch über Kabel und Verbindungskomponenten vernetzt. Danach werden auf Betriebssystemebene
- Ressourcen zur Nutzung auf Rechnern frei gegeben,
- Berechtigungen auf Betriebssystemebene definiert, die Regeln, welche Rechte Benutzer bzgl. der Nutzung einer Ressource haben,
- dem Administrator Werkzeuge zur Verwaltung der vernetzten Rechner zur Hand gegeben und
- der Zugriff auf Ressourcen geregelt.

Grundsätzlich existieren zwei grundlegende Netzwerkkonzepte um Computer auf Betriebssystemebene zu verbinden: **Peer-to-Peer- und Client/Servernetzwerke**. Unter Windows werden Peer-to-Peer-Netzwerke als **Arbeitsgruppe**, Client/Servernetzwerke als **Domäne** implementiert. Gegenüber einer Domäne hat eine Arbeitsgruppe folgende Nachteile:

- Es können maximal 10 Benutzer gleichzeitig auf eine Ressource zugreifen,
- Es existiert keine zentrale Verwaltungseinheit
- Ein Benutzer benötigt an jedem Rechner, an dem er sich anmelden möchte, ein Konto.

Der Vorteil einer Arbeitsgruppe gegenüber einer Domäne besteht darin, dass nicht zwingend ein Windows 2000 Server benötigt wird. Eine Serverlizenz ist wesentlich teurer als eine Professional-Lizenz.

Zum Aufbau einer Windows 2000-Domäne benötigt man zwingend Windows 2000-Server.

Aus oben genannten Gründen werden Arbeitsgruppen in der Praxis lediglich bei kleineren Netzwerken implementiert, z. B: in einer Anwaltskanzlei, in der drei Rechner vernetzt werden und lediglich drei Benutzer aktiv sind. Häufig wird als weiterer Vorteil einer Arbeitsgruppe genannt, dass die Verwaltung „einfacher“ sei, man weniger EDV-Kenntnisse bräuchte. Dieses Argument gilt nur bei einem sehr kleinen Netz. Wächst die Zahl der Rechner und die Zahl der Benutzer, so wird die Verwaltung einer Arbeitsgruppe im Vergleich zu einer Domäne aufwendiger.

Ferner erfordert der Einsatz bestimmter betriebswirtschaftlicher Anwendungssoftware (z. B. ERP-Systeme) oder bestimmter technischer Software (z. B. CAD-Systeme) ein Serverbetriebssystem.

Features einer Domäne

Eine Domäne in Windows 2000 ist eine logische Gruppierung vernetzter Computer. Eine Domäne stellt ein zentralisiertes Verfahren zum Verwalten von Netzwerkressourcen bereit. Der Benutzer des einen Computers kann auf die frei gegebenen Ressourcen auf anderen Computern in der Domäne zugreifen, sofern er über die entsprechenden Berechtigungen verfügt.
Vorteiler einer Domäne gegenüber Arbeitsgruppen:

- Einzelanmeldung
- Ein einziges Benutzerkonto
- Zentralisierte Verwaltung
- Skalierbarkeit

Aufbau einer Domäne

Um eine Domäne aufzubauen, werden PCs physisch vernetzt (z.B. über einen Switch). Danach wird auf einem PC mit sehr guter Hardwareausstattung ein Domänencontroller (DC) aufgebaut. Hierzu muss dieser mit Windows 2000 Server betrieben werden.

Achtung: Ein Rechner, der mit Windows 2000 Server betrieben wird, ist noch kein Domänencontroller.

Um einen Windows 2000 Server zum Domänencontroller aufzustufen, sind zwei Schritte erforderlich:

- Installation und Konfiguration des Dienstes DNS,
- Installation und Konfiguration von Active Directory

Die restlichen PC werden z. B. mit Windows 2000 Professional installiert und danach in die Domäne integriert. Beachte: Ein Rechner mit Windows 2000 Server kann normales Mitglied der Domäne sein und beispielsweise die Rolle eines Datei- oder Druckservers übernehmen.

Vorteile einer Domäne

- Organisatorische Objekte
- Einfaches Auffinden von Informationen
- Delegierte Verwaltungsrechte

Features von Active Directory

Ein Verzeichnisdienst hat die Aufgabe, die Ressourcen eines Netzwerks für alle Benutzer selektiv verfügbar zu machen.
Active Directory speichert Informationen über Netzwerkobjekte und stellt eine hierarchische Struktur bereit, die das Organisieren von Domänen und Ressourcen vereinfacht (-> einfache Suche für User).

- Organisiert Informationen
- Stellt eine zentrales Repository bereit
- Stellt Sicherheit bereit

Vorteile von Active Directory

- Geringere TCOs
- Flexible Verwaltung
- Skalierbarkeit
- Vereinfachte Verwaltung

Fazit: Eine Domäne ist ein Rechnerverbund, in dem die Ressourcen (bzw. Objekte) eines Netzwerkes und der Zugriff auf die Ressourcen in einer zentralen Einheit, dem Active Directory, (einem Verzeichnisdienst), verwaltet werden. Active Directory befindet sich auf einem bestimmten Rechner, dem so genannten Domänencontroller. Ein Domänencontroller muss mit einem Windows 2000 Serverbetriebssystem betrieben werden.

2. Netzwerk mit Windows 2000

2.1 Versionen des Win2k Servers

- Windows 2000 Server
  (Untersützt 4 Prozessoren; max. 4 GB Arbeitsspeicher; Funktionen zum Einsatz in kleinen und großen Unternehmen)
- Windows 2000 Advanced Server
- Windows 2000 Datacenter Server
- Windows 2000 AppCenter Server

2.2 Verzeichnisdienste

Aufgabe von Verzeichnisdiensten

Verzeichnisdienste haben die Aufgabe, die Ressourcen eines Netzwerks für alle selektiv verfügbar zu machen.

Active Directory

Das AD sind die Verzeichnisdienste in Win2k-Netzwerken. Beim AD handelt es sich um eine hierarchische und verteilte Datenbank. Sie basiert auf MS-Access-Datenbank-Funktionen.

- 1,5 – 20 Millionen Benutzer verwaltbar
- Delegierung von Verwaltungsaufgaben (auch Fernverwaltung) wird unterstützt
- Skalierbarkeit
- Flexibilität
- Interoperabilität
- Unterstützt alle Netzwerkstandards

2.3 Sicherheitsfunktion

Sicherheit durch die AD-Verzeichnisdienste

Der Verzeichnisdienst von Win2k gewährt die Sicherheit des Netzwerks auf der logischen Ebene. Zu den Prinzipien gehören Anmeldeauthentifizierung, Gruppenrichtlinien und Zugriffsberechtigungen.

2.4 Verwaltungsfunktionen

- Remote-Installationsdienste
- Gruppenrichtlinien
- Microsoft Management Console (MMC)
- Windows Scripting Host
- Telnet Server
- Windows Management Interface
- Terminal Services

2.6 Netzwerkinfrastruktur

DHCP

DHCP-Server vergeben an Workstations eindeutige IP-Adressen. Unter Win2k müssen DHCP-Server im AD autorisiert werden.

Ein DHCP-Server weist einem Rechner bei entsprechender Konfiguration beim Startvorgang eine IP-Adresse, eine Subnetzmaske, ggf. einen DNS-Server und ein Standardgateway zu. Dies ist z. B. beim Einsatz mobiler Rechner (z. B. Laptops) sinnvoll und vorteilhaft. Einem EDV-unkundigen Benutzer (z. B. einem Vertriebsmitarbeiter) wird dadurch die manuelle TCP/IP-Konfiguration erspart.
Darüber hinaus spielen DHCP-Server beim Zugang zum Internet eine wichtige Rolle, z. B. beim Zugang über einen DSL-Router.

DNS

Es ist Voraussetzung für die AD-Verzeichnisdienste. DNS unter Win2k unterstützt dynamische Aktualisierungen.
In der DNS-Datenbank werden außer der Zuordnung von Workstation-Namen zu IP-Adressen auch Informationen über die vorhandenen Netzwerkdienste gespeichert.

2.7 Dateiverwaltung, Dateisystem

Distribibuted File System

Das DFS ermöglicht, eine einzige Verzeichnisstruktur für die Datenbestände einer Organisation oder Abteilung oder der gesamten Firma zu erstellen.

Ordner, Dateien und sonstige Ressourcen können über das gesamte Netzwerk verteilt sein. Distributed Filesystem ermöglicht es einem Benutzer auf die verschiedenen Ordner und Dateien über einen Punkt (einem so genannten DFS-Stamm) zuzugreifen. Es entsteht durch DFS ein einzelnes virtuelles Dateisystem.

Datenträgerkontingente

Auf NTFS-Datenträgern können Sie die Speicherplatzbelegung verwalten. Hierzu wiesen Sie Benutzern Speicherplatz zu, den er dann zum Speichern seiner Daten verwenden kann.

3. Installation von Windows 2000 Server

3.1 Vorüberlegungen

Hardware-Voraussetzungen

Prozessor:	Pentium II mit 200 Mhz
Hauptspeicher:	128 MB
Festplattenlaufwerk:	650 MB freier Speicherplatz
Dateisystem:	NTFS

Voraussetzungen für die Installation

Installationsmethode:

Aktualisierung einer früheren WinNT-Version
- freier Speicherplatz ca. 650 MB
- Vollversion von Win2k Server oder die Update-Version

Vorteil: Bereits installierte Software wird ggf. automatisch erkannt und integriert Benutzerkonten, Benutzereinstellungen und die Konfiguration werden übernommen

oder

Neuinstallation
- freier Speicherplatz: min. 1 GB während der Installation, min. 100 MB nach der Installation
- Vollversion von Win2k Server

Nachteil: Ihre gesamte Software muss unter Win2k neu installiert werden

Weitere Fragen:

1. Soll der Server ein Dateiserver oder ein Domänencontroller sein?
   Abhängig von der Rolle (Dateiserver o. Domänencontroller) und dem Vorhandensein eines älteren Betriebssystems
2. Welches Dateisystem soll verwendet werden?
   Nur unter dem Dateisystem NTFS (New Technology File System) stehen die Sicherheitsmerkmale und der Verzeichnisdienst von Win2k zur Verfügung.
   Sie haben die Möglichkeit, Win2k in eine FAT-Partition zu installieren und diese Partition anschließend in eine NTFS-Partition umzuwandeln (Konvertierung).
3. Wie groß muss die Installationspartition sein?
   Für eine Neuinstallation von CD-ROM genügt ein Minimum von 685 MB, empfohlen werden jedoch 1 GB.
4. Welcher Lizensierungsmodus?
   - Pro-Arbeitsplatz-Lizenz
   - Pro-Server-Lizenz

3.2 Vorbereitungen

Welche Hardware-Komponenten sind im Rechner?
Wird in ein bestehendes Netzwerk installiert?
Installationsart wählen

- CD-ROM
  - Setup-Startdiskette: Setup-Start-Disketten können Sie mit Hilfe eines bereits installieren Rechners erstellen. Hierzu führen Sie an der Eingabeaufforderung den Befehl *Makeboot a:* aus dem Ordner Bootdisk der Win2k-CD aus.
- Über Netzwerk

4. Windows 2000 Server installieren

4.2 Einen Windows 2000 Server installieren

Der Aufbau eines neuen Win2k-Netzwerks beginnt immer mit der Installation eines ersten Servers. Dieser Server ist zu Beginn ein Datei- und Druckserver (Mitgliedserver), und er begründet eine Arbeitsgruppe.
Zum Domänencontroller wird der Server in einem späteren Schritt hochgestuft.

Installieren von Win2k über CD-ROM

Phase 1:

1. Windows 2000-Lizenzvertag
2. Zielpartition erstellen und formatieren
3. Datenträger überprüfen und Dateien kopieren

Phase 2:

1. Willkommen
2. Installation von Geräten
3. Gebietsschema
4. Benutzerinformationen
5. Lizensierungsmodi
6. Computername und Administratorkennwort
   Geben Sie den Computernamen (NetBIOS-Name) ein, mit dessen Hilfe die Station später im Netzwerk identifiziert werden soll. Vergeben Sie anschießend ein Kennwort für das lokale Konto des Administrators.
7. Windows 2000-Komponenten
8. Datum- und Uhrzeiteinstellungen
9. Netzwerkeinstellungen
10. Abschluss der Installation

4.3 Anmelden

Haben Sie die Installation als Neuinstallation durchgeführt und gehört der Computer keiner Domäne an, ist das Konto des lokalen Administrators das einzig gültige Konto.

5. Domain Name System

5.1 Domänennamespace

TCP/IP greift auf andere Computer ausschließlich über die IP-Adresse zu. Um die Adressierung für Benutzer zu erleichtern, sind Konzepte entwickelt worden, Computernamen IP-Adressen zuzuordnen. Zu diesen Konzepten gehören DNS und WINS.

Domain Name System

DNS ist das im Internet verwendete Konzept zur Namensauswertung. Es handelt sich um eine verteilte Datenbank. In einer hierarchischen Anordnung pflegen DNS-Server HOST-Dateien oder DNS-Datenbanken. Darin sind den Hostnamen IP-Adressen zugeordnet.

DNS-Domänennamen
Eine DNS-Domäne ist ein hierarchischer Namensraum für Computer, Dienste und DNS-Subdomänen eines Netzwerks. Die DNS-Domäne selbst besitzt auch einen Namen. Aus der Tatsache, dass eine Domäne eine oder mehrere Domänen der nächsten Ebene registriert, ergibt sich die Hierarchie. Die Namensräume sind hierarchisch angeordnet.
WICHTIG: Windows-Domäne ≠ DNS-Domäne

Hostnamen
Der komplette DNS-Name (Fully Qualified Domain Name: FQDN) für einen Host besteht aus dem Hostnamen und dem DNS-Domänennamen. Der FQD-Name gilt für alle im Computer installierten Netzwerkkarten: 1 Computer = 1 FQDN!

Beispiel:	Hostname:	pc1
	Netzwerkknoten:	marketing
	DNS-Domänenname:	marketing.teamup.de
	FQDN:	pc1.marketing.teamup.de

Virtuelle Hosts
Sind zwei oder mehr FQDNs für ein und denselben Computer (z. B. Internetserver) erforderlich, dann geht das nur über ein Hilfskonstrukt. Hierbei kreieren Sie trickreich so genannte virtuelle Hosts. Die Identifizierung eines Virtuellen Hosts schließlich führt wieder zum wahren FQDN des Computers.

Primäres DNS-Suffix
Der Bestandteil des FQDN, der vom DNS-Domänennamen gebildet wird, nennt man primäres DNS-Suffix. Jeder Computer muss ein primäres DNS-Suffix haben.
(Im Beispiel oben: marketing.teamup.de)

Hostname und Computername
Ein Host kann einen Hostnamen und einen Computernamen (NetBIOS-Name) besitzen. Die beiden Namen stimmen oft überein.

Richtlinien für die Erstellung des Domänennamespace
- Eine DNS-Struktur darf bis zu fünf Ebenen enthalten
- Eindeutige Namen für Subdomänen einer Domäne
- Die Verwendung von kurzen, aussagekräftigen Namen wird empfohlen
- Die maximale Länge des Domänennamens beträgt 63 Zeichen einschl. Punkte
- Gesamtlänge eines FQDN max. 255 Zeichen
- Die DNS-Standardzeichen sind: a-z, 0-9 und der Bindestrich
- Großbuchstaben werden automatisch durch Kleinbuchstaben ersetzt

5.2 Namensauflösung
Namensauflösung bezeichnet den Vorgang, bei dem ein DNS-Nameserver zu einer gegebenen IP-Adresse den zugehörigen Hostnamen ermittelt. Auch der umgekehrte Weg ist möglich.

Forward-Lookup
Zu einer IP-Adresse wird der zugehörige Hostname ermittelt

Reverse-Lookup
Zu einem Hostnamen wird die zugehörige IP-Adresse ermittelt

Client-/Servermodell der Namensauflösung
Die Namensauflösung folgt dem Client-/Servermodell.
Danach kann der DNS-Client Abfragen an den DNS-Nameserver schicken. Ein Nameserver kann nur solche Hostnamen und IP-Adressen auflösen, für die er autorisiert ist, d. h., für die er Einträge in seiner DNS-Datenbank besitzt. Erhält ein Nameserver eine Client-Abfrage, die er selbst nicht auflösen kann, übergibt er die Anfragen an einen übergeordneten DNS-Nameserver.

5.3 Dynamisches DNS

Dynamische Aktualisierung

Unter Win2k kann ein DNS-Client dem DNS-Server seinen Hostnamen und seine IP-Adresse mitteilen, wenn Hostname oder IP-Adresse des Clients geändert werden.
Computer die häufig an vers. Orten im Netzwerk aufgestellt werden, sollten im Idealfall ihre IP-Konfiguration über den DHCP-Dienst zugeteilt bekommen. Denn Dynamisches DNS und DHCP spielen so zusammen, dass die Zuordnung von Hostnamen zu IP-Adressen vom DHCP-Server an DNS mitgeteilt wird.

Sichere dynamische Aktualisierung

Sie ermöglicht, die dynamische Aktualisierung von Clients mittels Aktualisierungsrichtlinien zu reglementieren. Diese Funktion steht nur zur Verfügung in Zonen, die in AD integriert sind.

5.4 Zonen

Zonen und Zonendateien

Um die Netzwerklast und die Rechnerlast für ein DNS-Server zu verringern, wird der Domänennamespace in Zonen aufgeteilt.
Eine Zone kann umfassen:

- eine Domäne und eine Subdomäne
- eine einzelne Subdomäne
- einen Teil einer Domäne

Jede Zone hält die DNS-Namen von IP-Adressen in einer Zonendatei. Diese ist in der Zonendatenbank gespeichert.

Stammdomäne einer Zone

Die Stammdomäne einer Zone ist die Domäne, die innerhalb der Zone in der Hierarchie an oberster Stelle steht.

DNS-Stamm

DNS-Stamm eines Netzwerks ist die DNS-Domäne, die innerhalb des Netzwerks in der Hierarchie an oberster Stelle steht.
Der DNS-Server, der den DNS-Stamm pflegt, ist Stammnamensserver des Netzwerks.

Namesserver

Der Server, der die Zonendatenbank hält, ist DNS-Namesserver für die betreffende Zone. Er ist für diese Zone autorisierend. Jede Zone muss einen DNS-Nameserver haben. Ein Server aber kann DNS-Namesserver für mehrere Zonen sein.

Positionierung mehrerer Namesserver

Für jede Zone sollten nach Möglichkeit mehrere DNS-Namesserver zur Verfügung gestellt werden. Dabei ist einer der Namesserver ein primärer Namesserver (sekundäre Namesserver erhalten Kopien der primären Zonendatei).

5.5 Zonenübertragung

Replikation der Zonendatei

Die Zonendatei einer Zone wird primär auf die sekundären Namesserver kopiert. Der Informationsfluss erfolgt nur in diese Richtung. Dadurch wird die Zonendatei repliziert.
Außerdem kann für einen sekundären Namesserver Zonenübertragung von mehr als einem Masterserver konfiguriert werden. Damit kann man sicherstellen, dass ein sekundärer Namesserver auch dann die aktuellen Daten erhält, wenn einmal ein Masterserver ausfällt oder nicht erreichbar ist.

Replikationsmethoden

- Vollständige Zonenübertragung (AXFR)
- Inkrementielle Zonenübertragung (IXFR)

Veranlassung der Zonenübertragung

...durch den primären Namesserver

Der primäre Namesserver kann eine Zonenübertragung veranlassen. Wenn die Zonendaten geändert wurden, benachrichtigt der primäre den sekundären Namesserver über die Änderung.

...durch einen sekundären Namesserver

Auch ein sekundärer Namesserver kann die Zonenübertragung veranlassen. Er fragt den Namensserver nach Änderungen in der Zonendatei ab. Dabei sind Anlässe zur Abfrage des primären Namesservers:

- o das Starten des DNS-Serverdienstes auf dem sekundären Namesserver
- o der Ablauf des Intervalls für die Serveraktualisierung

5.6 Zonendeligierung

DNS-Subdomäne und deligierte Zone

Eine Subdomäne bleibt zunächst in der Zone der übergeordneten Domäne. Eine solche Zone nennt man „Subzone".
Erst durch das Deligieren einer Subzone an einen anderen als den bisherigen DNS-Server wird der Domänennamespace in mehrere Zonen aufgeteilt.

6. DNS-Dienst einrichten und konfigurieren

Schritte:

1. TCP/IP konfigurieren
2. DNS installieren
3. DNS konfigurieren

Anmerkungen:

- Damit ein Server den DNS-Dienst ausführen kann, muss er über eine konstante IP-Adresse verfügen.
- Im normalen Netzwerkbetrieb soll jeder DNS-Server sich selbst als DNS-Server verwenden.

DNS-Serverdienst testen

Nslookup ist ein Diagnoseprogramm, das zusammen mit dem Protokoll TCP/IP installiert wird. Verwenden Sie dieses Programm bevorzugt, um DNS-Server zu testen.

7. Einführung in Active Directory

Active Directory ist der Verzeichnisdienst von Windows 2000. Verzeichnisdienste haben die Aufgabe Ressourcen (z. B. eine Ordner, eine Datei, ein Drucker) eines Netzwerks Benutzern selektiv verfügbar zu machen. Sies stellen Funktionen zur Verfügung, mit denen Ressourcen eines Netzwerks organisiert und verwaltet werden können. Ferner überprüfen Sie den Zugriff auf eine Ressource durch einen Benutzer. Active Directory verwaltet alle Informationen über Objekte einer Domäne in einer Datenbank. Vorteile und Merkmale von Active Directory siehe Herdt, Kapitel 2.2.

Die Objekte einer Domänen können in Active Directory hierarchisch organisiert werden. Einzelne Objekte (z. B. die PC, die zu einer Abteilung gehören) werden in einer Organisationseinheit zusammengefasst. Organisationseinheiten können selbst wiederum zu Organisationseinheiten einer höheren Ebene zusammen gefasst werden (z. B. die Organisationseinheiten Produktionsplanung und Fertigung zur Organisationseinheit Produktion)

Mehrere Domänen können zu einer Struktur hierarchisch zusammen gefasst werden (z. B. Eine Domäne „asw" und eine Unterdomäne „wi").

Ein Objekt einer Domäne besitzt eine eindeutige Bezeichnung (GUID).

7.1 Grundlagen zu AD

Aufgaben von Verzeichnisdiensten

AD sind Verzeichnisdienste im Win2k-Netzwerk. Diese Netzwerkdienste erfüllen zwei Aufgaben:

- Auf der administrativen Seite stellen Verzeichnisdienste alle Funktionen zur Verfügung, mit denen die Ressourcen des Netzwerks organisiert, verwaltet und gesteuert werden können.
- Der andere Aspekt betrifft die Bereitstellung der Ressourcen für die Benutzer des Netzwerks.

Leistungsmerkmale von AD

- Zentrale Verwaltung aller Netzwerkressourcen durch eine einheitliche Verwaltungsschnittstelle
- Transparente Darstellung der Ressourcen für die Benutzer

Skalierbarkeit

In einem Win2k-Netzwerk können Millionen von Objekten verwaltet werden. Hierzu werden die Verzeichnisinformationen verteilt gespeichert. Das heißt, das Verzeichnis wird in Abschnitte unterteilt.

Unterstützte Standards

Das Ziel ist, die Navigation für Benutzer und Administratoren zu vereinfachen. Gleichzeitig soll der Zugriff auf die Ressourcen verschiedener Netzwerke – auch über das Internet – möglich sein. Dabei sollen Standorte und die verwendete Hardware und Betriebssysteme keine Rolle spielen.

- TCP/IP
- DNS u. DDNS
- LDAP u. LDIF
- KerberosV5
- X.509
- SNTP
- HTTP

7.2 Logische Struktur

Gruppentypen logischer Strukturen

Win2k bietet mit den AD-Verzeichnisdiensten ein Höchstmaß an Flexibilität. Diese Flexibilität wird dadurch erreicht, dass der logische Aufbau des Netzwerks vollkommen unabhängig von physischen Gegebenheiten wie z. B. der Netzwerktopologie ist. Jede denkbare Konstellation und Anforderung kann – in logischer Hinsicht – realisiert werden.

Entwurf für die Verzeichnisstruktur

Innerhalb der Verzeichnishierarchie werden Ressourcen logisch gruppiert.
Zur Beschreibung der logischen Struktur dienen folgende Komponenten:

- Objekt

  Ein Objekt steht für eine Netzwerkressource. Es ist die kleinste Einheit, die verwaltet werden kann. Jeder Vorgang im Netzwerk kann in letzter Konsequenz auf ein Objekt zurückgeführt werden.
  Ein Objekt ist beispielsweise ein Computer, ein Faxgerät, ein Benutzer, einer Druckerwarteschlange oder eine Richtlinie.

- Organisationseinheit

  Das Containerobjekt OU (Organizational Unit) dient dazu, Objekte zu gruppieren. So kann eine Organisationseinheit z. B. Benutzer, Benutzergruppen, Computer und andere Organisationseinheiten enthalten.
  Die Möglichkeit, eine Organisationseinheit in eine andere Organisationseinheit einzugliedern begründet die hierarchische Struktur der Verzeichnisdienste.

- Domäne

  Die Domäne ist die eigentliche und wesentliche Einheit von AD. Sie ist ein System, das sowohl nach innen als auch nach außen hin abgeschlossen ist. So werden beispielsweise im Verzeichnis einer Domäne nur die Informationen zu Objekten gespeichert, die in der Domäne enthalten sind. Auf der anderen Seite ist der Zugriff auf Objekte der Domäne von außen nur nach Anmeldung möglich.
  Eine Domäne hat ein Verzeichnis und dieses ist vollständig.
  Multimaster-Replikationsmodell
  Die Domänencontroller sind untereinander vollkommen gleichberechtigt. Dieses Prinzip unterscheidet sich grundlegend vom Prinzip der DNS-Namesserver.

Domänenmodi
Es gibt zwei versch. Modi, in denen Domänen betrieben werden können:
- gemischter Domänenmodus (mit NT-Rechnern)
- einheitlicher Domänenmodus (nur Win2k-Domänencontroller)

- Struktur

  Eine Struktur liegt vor, wenn Domänen hierarchisch angeordnet sind.
  Prinzipiell können Sie davon ausgehen, dass Domänen nur dann hierarchisch angeordnet werden, wenn Datenaustausch auch erwünscht ist. Oft geht eine hierarchische Struktur sogar aus einer einzelnen Domäne (Stammdomäne) hervor, dann nämlich, wenn ein Unternehmen wächst und das anfangs uniforme Netzwerk untergliedert wird. In diesem Sinne ist es auch zu verstehen, dass Vertrauensstellungen zwischen Domänen einer Struktur unter Win2k automatisch erstellt werden.
  - Hierarchie aus min. einer Domäne
  - Gemeinsames Namensschema
  - Fortlaufender Namespace

- Gesamtstruktur

  Die Einrichtung einer Gesamtstruktur kommt beispielsweise in Betracht, wenn Organisationen zusammengeführt werden oder Kooperationen eingehen und jede einen eigenen Internetdomänennamen innehat.
  - Hierarchie aus mind. einer Struktur
  - Vers. Namensschemata
  - Getrennter Namespace

  Zwar haben die Strukturen innerhalb einer Gesamtstruktur keinen gemeinsamen Namensraum, doch können die sowohl Ressourcen als auch administrative Aufgaben gemeinsam nutzen.

Vertrauensstellungen
Eine Vertrauensstellung beschreibt die Beziehung zwischen zwei Domänen. Die vertrauende Domäne lässt Anmeldeauthentifizierung aus der vertrauten Domäne zu.
- Unidirektionale, nicht transitive Vertrauensstellung (NT-Netzwerk)
- Bidirektionale, transitive Vertrauensstellung (reine Win2k-Netzwerke)

Konventionen für die Benennung von Objekten
- Eindeutige Namen (Distinguished Name, DN)
- Relative eindeutige Namen (Relative Distinguished Name, RDN)
- GUID (Globally Unique Identifier)
- UPN (User Principal Name)

7.4 Domänencontroller

Der Domänencontroller verwaltet alle sicherheitsrelevanten Interaktionen zwischen den Benutzern und der Domäne.
Replikation des AD-Verzeichnisses erfolgt unter den Domänencontrollern nach dem Mulitmaster-Replikationsmodell, bei dem alle Domänencontroller gleichberechtigte Peers sind. Dieses Konzept hat den Nachteil, dass zeitweise inkonsistente Daten existieren können. Durch Initiierung einer Replikation wird schließlich dafür gesorgt, dass die betreffenden Daten auf allen Domänencontrollern aktualisiert werden.
In AD werden aber auch Daten verwaltet, bei denen Dateninkonsistenz fatale Folgen haben würde. Für die Pflege und Verwaltung solcher Informationen muss auf die Multimasterreplikation verzichtet werden. Stattdessen übernehmen einzelne zu bestimmende Domänencontroller die Pflege dieser Daten.

Globaler Katalog
Im globalen Katalog werden bestimmte Attribute von Objekten gespeichert. Dabei handelt es sich um die Attribute, die oft bei Suchabfragen verwendet werden, wie z.B. Benutzernamen.
Positionierung:

- 1 globaler Katalog innerhalb einer Struktur; er ist gültig für alle Domänen dieser Struktur
- 1 globaler Katalog innerhalb einer Gesamtstruktur

Globaler Katalogserver:

Ein globaler Katalogserver speichert eine Kopie des globalen Katalogs und verarbeitet Suchabfragen. Ein globaler Katalogserver ist immer auch ein Domänencontroller. Globale Katalogserver spielen eine wichtige Rolle. Es muss ein Server des globalen Katalogs verfügbar sein, wenn sich ein Benutzer in der Domäne anmelden will.

Betriebsmaster
Betriebsmaster sind Domänencontroller, die bestimmte, einzelne Aufgaben und Vorgänge ausführen. Betriebsmater sind Einzelmaster; es darf kein weiter Domänencontroller mit gleichen Aufgaben vorhanden sein.

7.5 Integration von DNS in AD

AD-integrierte DNS-Zonen
Sind die Win2k-Domänenkontroller gleichzeitig DNS-Server, können die Zonen in AD integriert werden. Bei der Integration werden die Zonendaten aus der Zonendatei ausgelesen und im Verzeichnis gespeichert. Die Integration betrifft nicht die gesamte DNS-Zone, sondern immer nur die einzelne Textdatei auf dem betreffenden DNS-Server. Nach der Integration in AD werden die Zonendaten zusammen mit den Verzeichnisdaten über die AD-Replikation verteilt, aktualisiert und synchronisiert.

Vorteile der Integration von DNS mit AD

- Aktualisierung von Zonendaten nach dem Multimaster-Modell
- Vereinfachte Planung für den Netzwerkentwurf
- AD-Sicherheit für die Zonendaten
- Schnelle und effiziente Verteilung der Zonendaten

8. Active Directory installieren

8.2 Vorbereitungen

Benötigte Informationen über die Gesamtstruktur

- DNS-Domänennamen
- NetBIOS-Namen
- Domänenmodus

Voraussetzungen

- pro Domäne, mind. ein Win2k Server
- pro Server eine mind. 1 GB NTFS-Partition
- TCP/IP als Netzwerkprotokoll
- DNS-Server muss vorhanden sein
- Alle Domänencontroller müssen Systemzeit und Zeitzone ihrer geographischen Position entsprechen
- Bei Hinzufügen einer Domäne zu einer Gesamtstruktur o. Domänencontrollers zu einer vorhandenen Domäne müssen Anmeldeinformationen des Domänenadministrators bekannt sein

Assistent für die Installation von AD
Zur Installation oder Deinstallation von AD verwenden Sie das Programm Dcpromo.exe.
Durch das Installieren der Verzeichnisdienste wird der Win2k Server zu einem Domänencontroller hochgestuft.

Verzeichnisdienste deinstallieren
Sie haben die Möglichkeit, AD auch wieder zu deinstallieren. Dadurch wird der betreffende Domänencontroller zu einem Datei- und Druckserver herabgestuft.
WICHTIG: Beachten Sie jedoch, dass Sie die Domäne verlieren, falls Sie die Verzeichnisdienste vom einzigen Domänencontroller Ihrer Domäne entfernen!

Anmelden in der Domäne (nach Neustart bei Installation)
Windows hat ein neues Konto für den Domänenadministrator angelegt und dafür die Kennwörter vom Konto des lokalen Administrators verwendet. Der erste Domänenadministrator in einer neuen Struktur ist gleichzeitig verantwortlich für die gesamte Struktur, d. h. für die Firma bzw. für die Organisation. Er wird gelegentlich auch als Organisations- oder als Enterprise-Admin bezeichnet.
Der lokale Administrator existiert weiterhin. Anmelden an ein lokales Konto des Domänencontrollers ist im Normalbetrieb aber nicht mehr möglich. Künftig wird jede Anmeldung durch die Domäne autorisiert.

8.6 AD erkunden

Freigegebener Systemdatenträger
Jeder Domänencontroller ist Anmeldeserver. Die Dateien, die in der gesamten Domäne verfügbar sein müssen, werden im freigegebenen Verzeichnis SYSVOL gespeichert und vom File Replication Service auf die übrigen Domänencontroller repliziert.
Der Unterordner Scripts ist unter dem Namen NETLOGON freigegeben. Er enhält:
- Vorlagen für Gruppenrichtlinien
- Benutzerprofile und Anmeldeskripte

Die Ressourcen SYSVOL und NETLOGON werden vom Anmeldedienst netlogon verwendet, um Benutzeranmeldungen durchzuführen.

11. Active-Directory-Objekte

11.1 Objekt

Objekte
Das Objekt ist die kleinste Einheit, die verwaltet werden kann. Es besitzt einen Namen und einen Satz von Attributen.
- alles wird als Objekt betrachtet
- gesamte Verwaltung bezieht sich immer auf Objekte

Netzwerkressourcen
Jede Netzwerkressource wird durch Objekte repräsentiert. Netzwerkressourcen sind beispielsweise
- Geräte (Drucker)
- Dienste (Faxdienst)
- Datenbestände (Datenbanken)

Auch Elemente, die der Verwaltung eines Netzwerks dienen, sind Netzwerkressourcen, und in letzter Konsequenz auf Objekte zurückzuführen, z. B.:
- Benutzerkonten, Computerkonten
- Gruppen
- Organisationseinheiten
- Richtlinien

Aufgaben des Verzeichnisdiensts
- Gruppierung der Objekte in Container (Organisationseinheiten)
- Lokalisierung von Objekten
- Steuerung des Zugriffs auf die Netzwerkressource

11.2 Organisationseinheit

Definition
Das Containerobjekt OU (Organizational Unit) dient dazu, Objekte zu gruppieren. So kann eine Organisationseinheit z. B. Benutzer, Benutzergruppen, Computer und andere Organisationseinheiten enthalten.
Erforderliche Berechtigungen zum Erstellen und Verwalten einer OU: Domänenadministrator

11.3 Benutzerkonto

Bedeutung

- Authentifizierung des Benutzers
- Berechtigungen für Zugriffe auf die Netzwerkressourcen

Identifizierung

Der Benutzer wird über den UPN eindeutig identifiziert. Der UPN setzt sich zusammen aus dem Benutzeranmeldenamen und dem Domänennamen.

Sicherheitskennung

Ein Benutzerkonto besitzt eine Sicherheitskennung (Security Identifier, SID). Sie besteht aus einer Domänenkennung und einer relativen Kennung (RID).
Die SID ändert sich beispielsweise, wenn Die den Benutzer aus einer Domäne in eine andere Domäne verschieben. Der GUID dieses Benutzers jedoch bleibt gleich.

Organisieren von Benutzern

Sie können Benutzer auf der Ebene von Domänen ihrem Netzwerk hinzufügen. Um besser verwalten und die Verwaltung der Benutzer delegieren zu können, empfiehlt sich, den Benutzer einer Organisationseinheit oder einem Container zuzuordnen.

Benutzerprofil

Ein Benutzerprofil ist ein besonderes Verzeichnis. Das Profil wird beim Anmelden des Benutzers geladen.

Homeverzeichnisse werden in der Regel auf einem eigens dafür vorgesehenen Rechner, einem so genannten Dateiserver, erstellt. Aus Administrator- und Benutzersicht bietet ein Dateiserver Vorteile:

- Eine Sicherung der Dateien kann zentral erstellt werden.
- Unabhängig an welchem Rechner der Domäne sich ein Benutzer anmeldet, kann er auf seine Dateien zugreifen.

Serverbasierte Profile bieten den Vorteil, dass ein Benutzer unabhängig an welchem Rechner in der Domäne er sich anmeldet, immer die gleiche Arbeitsumgebung vorfindet.

Speicherort des Profils und Einflussnahme des Benutzers auf sein Profil

Das individuelle Benutzerprofil entsteht ausgehend vom Standardbenutzerprofil.

1) lokal gespeichert, veränderlich
2) serverbasiert, veränderlich
3) serverbasiert, verbindlich

Die Endung der Datei ntuser, die im Profilverzeichnis des Benutzers liegt, entscheidet darüber, ob er seine Arbeitsumgebung selbst verändern kann (veränderliches Benutzerprofil, ntuser.dat) oder ob er es nicht verändern kann (verbindliches Benutzerprofil, ntuser.man).

11.4 Computerkonto

Bedeutung

Auch Computer werden im AD mittels eines Objektes repräsentiert. Das logische Objekt ist das Computerobjekt. Computer sind schützenswerte Elemente eins Netzwerks. Jedes Computerkonto besitzt eine SID.

Organisieren von Computern

Sie können Computer auf der Ebene von Domänen Ihrem Netzwerk hinzufügen (Verwaltung: wie Benutzer).

12. Active-Directory-Objekte verwalten

Vordefinierte Container in einer Domäne

- Bulitin — Vordefinierte Gruppen für die vers. Aufgabenbereiche bei der Verwaltung eines Netzwerks
- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- Users

Autorisierte Personen

Auf Dauer ist das Hinzufügen von Workstations zur Domäne nicht die Aufgabe von Domänenadministratoren. Sie werden beim Aufbau eines Netzwerks als frühzeitig einen oder mehrere Personen zu Kontenoperatoren bestimmen oder eine geeignete Objektverwaltung einrichten.

13. Gruppen

Über Benutzerkonten werden in einer Domäne ebenso wie in einer Arbeitsgruppe Berechtigungen an Ressourcen vergeben.
Domämenbenutzer werden im Active Directory verwaltet (Snap-In AD Benutzer und Computer).
Meldet sich ein Benutzer an einem Client der Domäne an, so werden die Eingabedaten im Active Directory des Domänenbenutzers authentifiziert. Bei erfolgreicher Anmeldung erhält der Benutzer eine Art Zugriffsticket für den Zugriff auf Ressourcen innerhalb der Domäne.

Besteht ein Netzwerk auf Betriebssystemebene aus mehreren Domänen, so können Benutzer einer Domäne A auf Ressourcen einer anderer Domäne B zugreifen, falls sich die Domänen vertrauen und der Benutzer aus Domäne A die entsprechende Zugriffsberechtigung für die Ressource in Domäne B besitzt. Berechtigungen über Domänen hinweg werden über Domänenbenutzergruppen vergeben. Es existieren dabei drei Arten von Domänenbenutzergruppen: Domänenlokale, globale und universelle Gruppen. Domänenlokale und universelle Gruppen können dabei Benutzer und Gruppen anderer Domänen beinhalten.

13.1 Gruppentypen

Sicherheitsgruppe

Mit Sicherheitsgruppen steuern Sie den Zugriff auf Ressourcen, indem Sie Berechtigungen zuweisen oder entziehen.

Verteilergruppen

Für Aufgaben, die keine Sicherheitsrelevanten Aspekte haben, können Sie Verteilergruppen definieren. Einer Verteilergruppe können Sie jedoch keine Berechtigungen erteilen. Verteilergruppen werden Sie in der Praxis eher selten erzeugen.

13.2 Gruppenbereiche

Sicherheits- und Verteilergruppen werden charakterisiert nach folgenden Bestimmungen:

- Herkunft der Gruppenmitglieder
- Wirkungsradius des Zugriffs

Arten:

- Universale Gruppe
- Globale Gruppe
- Domänenlokale Gruppe

  Domänenlokale Gruppen werden meist einfach nur “lokale Gruppen” genannt. Sie müssen aber die domänenlokale Gruppe von der lokalen Gruppe, die es auf Arbeitsgruppencomputern gibt, unterscheiden.

Einschränkungen bei universalen Gruppen

Die Verwendung von universalen Gruppen wirkt sich auf die Netzwerkleistung aus:

- vergrößern den globalen Katalog
- Ändern von Mitgliedschaften erfordert replizieren des globalen Katalogs
- Zugriffstoken ist größer

Empfehlungen:

- Beschränken Sie den Einsatz von universalen Gruppen auf die Fälle, in denen Zugriffe auf mehrere vers. Ressourcen in vers. Domänen gewährt werden sollen.
- Machen Sie globale Gruppen zu Mitgliedern in der universalen Gruppe und nicht einzelne Benutzer

13.3 AGDLP-Regel

Um Benutzern einer Domäne den Zugriff auf eine Ressource einer anderen Domäne zu gewähren, verwendet man aus Effizienzgründen eine bestimmte Vorgehensweise, die so genannte AGDLP-Regel. Um z. B. einem Benutzer aus der Domäne „wi“ den Zugriff auf einen Ordner „Berichte“ in der Domäne „asw“ zu ermöglichen, fügt man den Benutzer in eine globale Gruppe „teilprojekt_wi“ ein. In der Domäne „asw“ erzeugt man eine domänenlokale Gruppe „projekt“ und fügt in diese Gruppe die Gruppe „teilprojekt_wi“ aus der Domäne „wi“ als Mitglied ein. Über die Gruppe „projekt“ definiert man jetzt die Zugriffsberechtigung auf den Ordner „berichte“.

Regel

1. Schritt
   Im ersten Schritt erhält der Benutzer (A = Access) Mitgliedschaft in einer Globalen Gruppe (G = Global Group).
2. Schritt
   Im zweiten Schritt wird die globale Gruppe in eine lokale Gruppe (DL = Domain Local Group) platziert.
3. Schritt
   Im dritten Schritt erfolgt die Vergabe von Zugriffsberechtigungen (P = Permission) an die lokale Gruppe

15. Berechtigungen und Objektverwaltung

Um eine Ressource auf einem PC von einem anderen PC der Domäne aus zu nutzen, sind die gleichen Arbeitsschritte erforderlich wie in einer Arbeitsgruppe. Nach Erstellung einer Ressource, wird diese frei gegeben. Danach kann man für diese Zugriffsberechtigungen für Benutzer und Gruppen definieren. Hierfür stehen wie in der Arbeitsgruppe Freigabe- und NTFS-Berechtigungen zur Verfügung.

Für jedes Objekt wird in einer Domäne eine Access Controll List (ACL) verwaltet, die die Zugriffsberechtigungen verwaltet.

Welche Berechtigungen sich für einen Benutzer ergeben, ergibt sich aus nachfolgenden Regeln:

1. Der Benutzer „Jeder“ ist ein stellvertretener Name, der für jeden Benutzer gültig ist. Jeder Benutzer gehört der Gruppe „Jeder“ an. Standardmäßig ist für diesen Benutzer „Vollzugriff zugelassen“. Dies bedeutet, dass das hier ausgewählte Objekt im Vollzugriff liegt bzw. der Zugriff nicht eingeschränkt ist.
2. Die tatsächlichen Berechtigungen eines Benutzers für eine Ressource setzen sich **kumulativ** aus allen Berechtigungen zusammen, die er aufgrund seiner Mitgliedschaft in verschiedenen Gruppen besitzt.
3. **Verweigerungen schlagen Zulassungen**! Besitzt ein Benutzer für ein bestimmtes Objekt eine Zulassung (z. B. über Gruppenmitgliedschaften) und eine Verweigerung, so besitzt der Benutzer effektiv eine Verweigerung.
4. Werden für einen Benutzer weder Berechtigungen noch Zulassungen markiert, so werden die Berechtigungen von der oder den Gruppen übernommen, denen der jeweilige Benutzer angehört. Werden die Berechtigungen auch nicht über eine Gruppe definiert, werden dem Benutzer sämtliche Berechtigungen entzogen.

5. NTFS-und Freigabeberechtigungen werden normalerweise vom übergeordneten Verzeichnis, in dem sie eingerichtet worden sind, an alle Unterverzeichnisse und Dateien weitergegeben, d. h. vererbt. Die Vererbung kann jedoch bei NTFS-Berechtigungen auf Datei- oder Unterordnerebene aufgehoben werden.
6. Freigabeberechtigungen sind nur bei Zugriff auf eine Ressource über das Netzwerk wirksam. NTFS-Berechtigungen sind bei Zugriff über das Netzwerk und bei lokalem Zugriff wirksam.
7. Sind für eine Ressource sowohl NTFS- als auch Freigabeberechtigungen definiert, so werden potentielle Konflikte dadurch aufgelöst, dass die den Zugriff am meisten einschränkende Berechtigung gewinnt.

15.1 Berechtigungen

Zugriffssteuerung

Für jedes Objekt wird im AD eine Liste mit Zugriffsberechtigungen verwaltet. Diese Liste heißt Discretionary Access Control List (DACL). In dieser Liste wird vermerkt, welcher Benutzer auf das Objekt oder seine Attribute zugreifen kann und welche Aktionen im Einzelnen der jeweilige Benutzer ausführen darf.
Mit Hilfe der AD-Berechtigungen können Sie einem einzelnen Benutzer oder einer Benutzergruppe die Möglichkeit geben, Objekte zu verwalten:

- Organisationseinheit
- Organisationseinheit und die untergeordneten OUs
- Einzelnes Objekt

Benutzer haben standardmäßig keine Möglichkeit, auf ein neu erstelltes Objekt zuzugreifen. Erst wenn ein Administrator oder ein Besitzer des Objektes Berechtigungen für den Objektzugriff zuweist, können Benutzer mit der betreffenden Ressource arbeiten.

Direkte Steuerung des Zugriffs

Direkte Steuerung des Zugriffs bedeutet, dass Sie auf der einen Seite ein Objekt haben und auf der anderen Seite einen Berechtigten und festlegen, welcher Zugriff erlaubt sein soll. Berechtigte können sein:

- Benutzer
- Benutzergruppe
- Computer

Hier haben Sie zwei Möglichkeiten, den Zugriff zu steuern:

- Zugriff gewähren
- Zugriff verweigern

Indirekte Steuerung des Zugriffs

Berechtigungen können vererbt werden. Das bedeutet, dass ein Benutzer Zugriff auf ein Objekt bekommt, ohne dass diesen Zugriff für ihn explizit erteilen.

Effektive Berechtigungen

Welche Berechtigungen ein Benutzer tatsächlich auf das Objekt hat, ergibt sich aus der Summe aller Berechtigungen, die ihm

- direkt gewährt oder verweigert und
- durch Vererbung zuteil oder entzogen werden.

(Restriktiver Charakter der Zugriffsverweigerung)

Empfehlungen für die Vergabe von Berechtigungen

Gewährende Berechtigungen:	Weisen Sie gewährende Berechtigungen nach Möglichkeit immer Gruppen zu und nicht einzelnen Benutzern.
Verweigernde Berechtigungen:	Verweigernde Berechtigungen sollten Sie dagegen bevorzugt einzelnen Benutzern zuweisen.
Vollzugriff:	Es sollte nach Möglichkeit immer eine Benutzergruppe oder ein Benutzer den Vollzugriff auf ein Objekt haben. Auch ein Administrator kann ein Objekt, wenn er den Vollzugriff selbst nicht innehat, in vollem Umfang nicht verwalten!

15.2 Vererbung con Berechtigungen

Übertragung von Berechtigungen

Berechtigungen können ausgehend vom übergeordneten Objekt auf untergeordnete Objekte übertragen werden. Die Vererbung wird jeweils für das untergeordnete Objekt festgelegt.

Standardeinstellungen für die Berechtigungsvererbung

Die Berechtigungsvererbung ist für alle Objekte standardmäßig aktiviert!

Vererbung von Berechtigungen verhindern

Sie haben die Möglichkeit, die Vererbung auszuschließen. Die Konfiguration nehmen Sie jeweils am betreffenden untergeordneten Objekt vor.

- Vererbung von Berechtigungen für ein Objekt komplett unterbinden
- Einzelne Berechtigungen ausschalten

15.3 Objektverwaltung

Delegierung der Objektveraltung

Sie haben die Möglichkeit, einzelne Benutzer oder Benutzergruppen mit der Verwaltung von Objekten zu betrauen. Jedoch ist es wenig sinnvoll, Verwaltungsaufgaben einzelner Objekte zu erteilen.
Delegierbare Verwaltungsaufgaben:

- Objekte erstellen, bearbeiten, löschen
- Spezielle Berechtigungen für Attribute von Objekten bearbeiten

15.4 Verwaltungstools für die Objektverwaltung

Microsoft Management Console (MMC)

Die MMC ist ein Instrument, mit dem Sie mehrere Verwaltungsprogramme (Snap-Ins) in einer Platform (Konsole) zusammenstellen können. Damit können Sie Werkzeuge (Konsolen) für häufig durchzuführende Verwaltungsaufgaben individuell erstellen.
Konsolen sind Dateien mit der Dateinamenerweiterung MCS.
Eine Konsole kann nur verwendet werden, wenn die betreffenden Verwaltungsprogramme auf dem Computer auch installiert sind.

Konsolenmodi

Autorenmodus:	Das bedeutet das derjenige, der die Konsole öffnen darf, den Vollzugriff auf die Konsole hat.
Benutzermodus:	Für die Delegierung der Objektverwaltung empfiehlt sich, Konsolen zu erstellen und zu verteilen, die von der betreffenden Person nicht mehr verändert und auch nicht gespeichert werden können.

15.5 Objektbesitz

Besitzer

Alle AD-Objekte haben jeweils einen Besitzer. Dabei gilt das Verursacherprinzip: Besitzer eines Objekts ist derjenige, der es erzeugt hat.

Berechtigungen

Der Besitzer eine Objekts kann Berechtigungen auf das Objekt vergeben, er kann sogar Admins den Zugriff auf das Objekt verwehren. Sie haben jedoch als Admin jederzeit die Möglichkeit, den Besitz am Objekt wieder zu übernehmen. Danach können Sie das Objekt wieder umfassend verwalten.

Besitzerwechsel

Damit der Besitz an einem Objekt auf eine andere Person übergehen kann, muss der Besitzer der betreffenden Person die Berechtigung erteilen, den Besitz am Objekt zu übernehmen. Anschließend ist noch erforderlich, dass die betreffende Person selbst den Besitz am Objekt tatsächlich auch übernimmt.
Es ist nicht möglich, dass ein Besitzer einer anderen Person den Besitz am Objekt überträgt.
Eine Ausnahme bzw. Besonderheit stellen die Admins dar:

- Ein Admin kann den Besitz an einem Objekt jederzeit übernehmen. Besitzer wird jedoch nicht der einzelne Admin selbst, sondern die Gruppe Domänen-Admins. Damit ist gewährleistet, dass beispielsweise beim Weggang eines Mitarbeiters dessen Dateien weiterhin dem Unternehmen zur Verfügung stehen.
- Der Besitz an einem Objekt kann zwischen den vers. Admin-Gruppen oder auf einen einzelnen lokalen Admin übertragen werden, ohne dass eine Besitzübernahme nötig ist.

17. Datei- und Druckdienste

17.1 Freigeben und Veröffentlichung von Dateien und Druckern

Freigabe

Damit Benutzer über das Netzwerk auf Ordner oder Drucker zugreifen können oder Netzlaufwerksverbindungen zu Ordnern herstellen können, muss ein solcher Ordner oder der Drucker freigegeben werden. Darüber hinaus muss der Benutzer auch die Berechtigungen zum Zugriff innehaben.
Mit einer Freigabe sind gleichzeitig auch Freigabeberechtigungen zu definieren (Vollzugriff, Ändern, Lesen).
Freigaben sind Voraussetzung dafür, dass ein Zugriff über das Netzwerk überhaupt möglich ist. Freigabeberechtigungen schränken nur die Zugriffe, die über das Netzwerk erfolgen, ein.

Das Snap-In Computerverwaltung

Zur Verwaltung von Freigaben verwenden Sie das Snap-In Computerverwaltung.

Veröffentlichung von Dateien und Druckern in AD

Sie haben die Möglichkeit, freigegebene Ordner, Drucker oder andere Netzwerkressourcen im AD zu veröffentlichen. Dies hat den Vorteil, dass die Netzwerkressourcen für die Benutzer leichter aufzufinden sind als Freigaben. Um einen freigegebenen Ordner zu finden, muss der Benutzer wissen, auf welchem Server der Ordner gespeichert ist.

17.2 NTFS-Berechtigungen

Steuerung des Zugriffs auf Objekte

- AD-Berechtigungen
- Freigabeberechtigungen
- NTFS-Berechtigungen

Manche Objekte werden nur durch AD-Berechtigungen geschützt z. B. Benutzer, Gruppen, Kontakte. Andere Objekte werden außer durch AD-Berechtigungen auch durch NTFS-Berechtigungen geschützt, z. B. Ordner, Dateien, eine Druckwarteschlange. Manche davon werden außerdem durch Freigabeberechtigungen geschützt, z. B. freigegebene Ordner.

Standardmäßige und spezielle NTFS-Berechtigungen

Für Dateien, Ordner und Druckwarteschlangen können NTFS-Berechtigungen definiert werden. Tatsächlich setzt Windows NTFS-Berechtigungen beim Erstellen eines solchen Objekts automatisch und mit solchen Einstellungen, die der normalen Nutzung des betreffenden Objekts entspricht.
NTFS-Berechtigungen schränken nicht nur die Zugriffe ein, die über das Netzwerk erfolgen, sondern auch solche, die von lokal aus auf den Ordner ausgeführt werden.
NTFS-Berechtigungen werden standardmäßig auf untergeordnete Objekte vererbt.
NTFS-Berechtigungen sind bis ins Kleinste augeschlüsselt (spezielle Berechtigungen). Doch gibt es so genannte standardmäßige NTFS-Berechtigungen. Das bedeutet, dass mehrere einzelne spezielle NTFS-Berechtigungen so zusammengefasst werden, dass sich aus der Summe dieser Berechtigungen schließlich eine sinnvolle Zugriffsart ergibt.

Verwaltung des Objektbesitzes

Der Besitzer eines Objekts kann von einem Benutzer oder einer Benutzergruppe auf einen anderen Benutzer oder eine andere Benutzergruppe übergehen. Hierfür sind zwei Aktionen erforderlich:

1. Schritt: Berechtigung für Benutzer oder Benutzergruppe
2. Schritt: Explizite Übernahme des Besitz durch Berechtigten

Eine besondere Bedeutung kommt der Gruppe der Admins zu: Diese Gruppe kann jederzeit den Besitz an einem Objekt übernehmen, selbst wenn der momentane Besitzer die Besitzübernahme durch Admins ausgeschlossen hat. Damit ist gewährleistet, dass Dateien auch nach dem Ausscheiden eines Mitarbeiters dem Unternehmen weiterhin zur Verfügung stehen.

Vererbung von NTFS-Berechtigungen

NTFS-Berechtigungen werden standardmäßig auf untergeordnete Ordner und Dateien vererbt!

17.3 Distributed File System

Logische Verzeichnisstruktur
Das verteilte Dateisystem (DFS) stellt ein einzelnes Dateisystem dar. Dieses Dateisystem ist hierarchisch aufgebaut. Die Ordner und sonstigen Ressourcen können über das gesamte Netzwerk verteilt sein.

Erleichterte Fernverwaltung
Mit Hilfe des DFS können Admins Dateiressourcen leichter fernverwalten. Es ist möglich auf alle Freigaben über einen einzigen Punkt zugreifen und diese verwalten.

Struktur von DFS
Den Ausgangspunkt im DFS bildet der DFS-Stammknoten. Er steht in der Hierarchie der logischen Verzeichnisstruktur an oberster Stelle. Einem DFS-Stammknoten können weitere Knoten untergeordnet sein. Jeder Knoten im DFS verweist auf einen freigegebenen Ordner. Die einzelnen freigegebenen Ordner wiederum sind auf den vers. Servern an vers. Standorten gespeichert.

Steuerung des Benutzerzugriffs
Zugriffsberechtigungen im Sinne von Beschränkungen werden im DFS nicht vergeben. Sie sind auch nicht erforderlich, denn die Steuerung des Zugriffs erfolgt allein auf der Grundlage der Freigabe- und NTFS-Berechtigungen der tatsächlichen vorhandenen – also der physischen – Ordner.

Ordner Freigeben

Die Berechtigungsfilter Freigabeberechtigungen und NTFS-Berechtigungen sind standardmäßig so eingestellt, dass Zugriffe durch Benutzer nicht beschränkt werden. Im Einzelnen sind dies:

- Freigabe – Jeder – Vollzugriff
- NTFS – Jeder – Vollzugriff zugelassen (geerbt)

Beachten Sie, dass – insbesondere, wenn NTFS-Berechtigungen auf Festplattenebene bereits beschränkt worden sind – die Standardeinstellung nicht mehr gültig ist. Welche Zugriffe im Einzelnen gewährt sind, resultiert dann aus den NTFS-Berechtigungen, die vom übergeordneten Ordner geerbt wurden oder die im aktuellen Ordner explizit definiert wurden.

20. Gruppenrichtlinien

Gruppenrichtlinien sind Regeln, die vom Administrator für die Benutzer und Computer eines Netzwerks aufgestellt werden. Richtlinien dienen dazu den Spielraum für Benutzer gegenüber der Standardinstallation einzuschränken oder zu erweitern.

Beispiele:

- Die Kennwörter aller Domänenbenutzer sollen mindestens 8 Zeichen lang sein.
- Nach drei gescheiterten Anmeldeversuchen wird das Benutzerkonto gesperrt.
- Nach Abmeldung des Benutzers soll automatisch der Papierkorb geleert werden.
- Verteilung von bestimmter Software über das Netzwerk.
- Überwachung des Objektzugriffs (z. B. eines Ordners) durch einen Benutzer.

Grundlagen:
In einer Domäne werden Gruppenrichtlinien in Form von sogenannten Gruppenrichtlinienobjekten gespeichert. Ein Objekt enthält eine Menge von einzelnen Richtlinien. Gruppenrichtlinienobjekte sind an Active Directory-Container (z. B. Organisationseinheiten, Domänen) geknüpft.

Es gibt vier Container, für die Gruppenrichtlinien erstellt werden:

- Lokale Gruppenrichtlinien an einem lokalen Rechner,
- Gruppenrichtlinien für die Domäne,
- Gruppenrichtlinien für Organisationseinheiten.
- Gruppenrichtlinien für Standorte (diese werden wir nicht behandeln).

Für einen Container können mehrere Gruppenrichtlinienobjekte definiert werden.

Gruppenrichtlinien werden standardmäßig vererbt. Ein mit einem bestimmten Active Directory-Container verbundenes Gruppenrichtlinienobjekt wird auf alle untergeordneten Container vererbt.
Die standardmäßige Vererbung kann jedoch aufgehoben werden.
In einer Domäne Richtlinien können sich auf eine Domäne, eine Organisationseinheit oder auf einen lokalen Rechner beziehen.

Wir kennen Richtlinien bereits von Windows 2000 Professional. Über die MMC konnte ein Snap-In für Richtlinien gestartet werden. In diesem Snap-In konnte man dann diverse Einstellungen vornehmen. Bei einem solchen Snap-In handelt es sich um ein Gruppenrichtlinienobjekt. Auf Ebene einer Domäne können mehrere Richtlinienobjekte definiert werden. Ein Richtlinienobjekt wird dabei mit einer Domäne oder einer Organisationseinheit verknüpft, auf das es sich auswirken soll.

Aufbau und Elemente eines Gruppenrichtlinienobjekts
Ein Gruppenrichtlinienobjekt umfasst eine Menge von Richtlinien. Diese werden in zwei Kategorien unterteilt:
Richtlinien der
- Computerkonfiguration und der
- Benutzerkonfiguration.

Die Richtlinien der Computerkonfiguration können Registry-Einträge innerhalb von HKEY_LOCAL_Machine beeinflussen. Diese Einstellungen werden immer für einen Computer angewendet, ungeachtet dessen, welcher Benutzer sich anmeldet.

Die Richtlinien der Benutzerkonfiguration können Registry-Einträge innerhalb von HKEY_LOCAL_USER beeinflussen. Die Richtlinien der Benutzerkonfiguration gelten für jeden Computer, an dem sich der Benutzer anmeldet.

Verarbeitung von Gruppenrichtlinien:
- Bei der Anmeldung eines Computers in der Domäne werden die Einstellungen der Computerkonfiguration aus den geltenden Gruppenrichtlinienobjekten ausgelesen und umgesetzt.
- Bei der Anmeldung eines Benutzers werden die Einstellungen des Benutzerkonfigurationsabschnitts der Gruppenrichtlinien auf die Umgebung des Benutzers angewendet.

Die Richtlinienobjekte werden in der nachfolgenden Reihenfolge abgearbeitet:
- Lokales Gruppenrichtlinienobjekt,
- Gruppenrichtlinienobjekt für den Standort,
- Gruppenrichtlinienobjekt für die Domäne,
- Gruppenrichtlinienobjekt für die Organiationseinheit gemäß der vorliegenden Hierarchie.

20.1 Einsatzbereiche von Gruppenrichtlinien

Definition
Gruppenrichtlinien sind Konfigurationsanweisungen. Mit Richtlinien können Sie bestimmte Einstellungen erzwingen. Sie werden – je nach Art – auf einen Standort, die Domäne oder eine Organisationseinheit angewendet. Sie beinhalten auch die Funktion der Vererbung und die Möglichkeit, die Verwaltung zu delegieren. Gruppenrichtlinien werden im AD gespeichert und auf dem Wege der Replikation domänenweit verfügbar gemacht.

Vorteile von Gruppenrichtlinien
Allg. gesprochen, verwenden Sie Gruppenrichtlinien, um Desktops von Benutzern und Computer zu konfigurieren. Sie helfen, die Gesamtbetriebskosten eines Netzwerks zu senken, indem die Produktivität von Mitarbeitern auf einem hohen Niveau gehalten wird.
Gruppenrichtlinien sind ein mächtiges Instrument zur Konfiguration, Verwaltung und Absicherung eines Netzwerks. Es kann nicht hoch genug eingeschätzt werden:
- Handlungsmöglichkeiten von Benutzern beschränken
- Aufrechterhaltung von Computerkonfigurationen
- Pflege und Verfügbarkeit der verwendeten Anwendungsprogramme im Unternehmen
- Verwaltungsaufwand der Administratoren senken

Einsatzbereiche
- Registrierungseinträge überschreiben
- Domänensicherheit
- Skriptverarbeitung
- Software-Installation
- Remote-Installation
- Ordnerumleitung

20.2 Gruppenrichtlinienobjekt
Im Gruppenrichtlinienobjekt (Group Policy Object, GPO) werden die einz. Gruppenrichtlinien (Gruppenrichtlinieneinstellungen) gespeichert. Der Inhalt des Gruppenrichtlinienobjekts wird sowohl in einer Vorlage als auch einem Container gespeichert.

Gruppenrichtlinienvorlage
Gruppenrichtlinienvorlagen (Group Policy Template, GPT) speichern alle Gruppenrichtliniendaten eines GPOs die sich auf administrative Vorlagen, Skripts, Ordnerumleitung, Software und Sicherheit der Domäne beziehen.
Gruppenrichtlinienvorlagen werden im Ordner SYSVOL auf dem Domänencontroller gespeichert und durch die AD-Replikation anschließend domänenweit verteilt. Jedem Gruppenrichtlinienobjekt entspricht hier ei Ordner in der Ordnerhierarchie. Der Ordner selbst trägt nicht den Namen des GPOs, sondern wird mit dem GUID benannt.

20.3 Verarbeitung der Gruppenrichtlinieneinstellungen
Reihenfolge bei Verarbeitung von Gruppenrichtlinien
Der Computer startet...
1. Lokale Gruppenrichtlinie
2. Startskripts
3. Liste der GPOs (Computer)

Der Anmeldedialog erscheint, der Benutzer meldet sich an.
4. Benutzerprofil
5. Liste der GPOs (Benutzer)
6. Anmeldeskripts

Die Benutzeroberfläche erscheint.

Aktualisierung von Gruppenrichtlinieneinstellungen
Konfigurationen, die durch Gruppenrichtlinien gesetzt werden, werden in regelmäßigen Abständen aktualisiert. Das Intervall beträgt für Client-Computer ca. 90 Minuten, bei Domänencontrollern etwa 5 Minuten.

20.4 Gruppenrichtlinienberechtigungen
Anwendung von Gruppenrichtlinien auf Benutzergruppen
Die kleinste Einheit, die mit einem GPO verknüpft werden kann, ist die OU. Möchten Sie dass ein GPO nicht für alle Benutzer einer OU, sondern nur für bestimmte Benutzer gültig sein soll, erstellen Sie eine Sicherheitsgruppe in der OU. Anschließend können Sie dieser Sicherheitsgruppe die Berechtigungen zum Lesen und Übernehmen des Gruppenrichtlinienobjekts zuweisen.

20.5 Vererbung von Gruppenrichtlinien
Standardmäßige Vererbung
Gruppenrichtlinien werden innerhalb der Domäne standardmäßig vererbt. Eine Gruppenrichtlinie, die Sie mit einer Domäne verknüpft haben, wird an alle Organisationseinheiten der Domäne vererbt.
Eine Sonderstellung bilden die Gruppenrichtlinien, die Sie mit einem Standort verknüpfen. Sie gelten für alle Computer am Standort. Das GPO selbst jedoch wird nur in einer Domäne gespeichert.

Reihenfolge der Vererbung
1. GPOs des Standorts
2. GPOs der Domäne
3. GPOs der OU gemäß der Hierarchie

Für den Benutzer sind die Richtlinien der OU, zu der er gehört, in jedem Fall wirksam. Die überschreiben nämlich solche Konfigurationen, die weiter oben in der Hierarchie möglicherweise gesetzt wurden, sofern sie sich auf denselben Sachverhalt beziehen.

22 Gruppenrichtlinien einsetzen

22.1 Gruppenrichtlinienimplementierung planen

Schritte bei der Planung einer Gruppenrichtlinienimplementierung

1. Schritt:
   Die Planung einer Gruppenrichtlinienimplementierung beinhaltet immer das Heraussuchen und die Bewertung von geeigneten Richtlinieneinstellungen, die in ihrer Gesamtheit die gewünschten Einschränkungen erzielen. Oft ist es so, dass eine Einschränkung, die auf den ersten Blick lapidar erscheint, nur durch das Zusammenwirken mehrerer einzelner Richtlinien effektiv erzielt werden kann.
2. Schritt:
   Sie müssen dann festlegen, mit welchem Standort oder welcher OU das Gruppenrichtlinienobjekt zu verknüpfen ist und ob das GPO auf untergeordnete Einheiten vererbt werden soll.
3. Schritt:
   Sie müssen festlegen, ob die Vererbung von Gruppenrichtlinien in einer OU der Hierarchie auszuschließen ist. Außerdem müssen Sie festlegen, ob die Richtlinieneinstellungen eines GPO mittels der Option KEIN VORRANG durchgesetzt werden soll.

Backupdomänencontroller

Fällt der Domänencontroller einer Domäne aus, so stehenden Benutzern Netzwerkdienste nicht mehr zur Verfügung. Dadurch sinkt die Produktivität der Benutzer. Um dieses Problem zu umgehen, kann man in die Domäne einen Backupdomänencontroller (BDC) einfügen, der als Stellvertreter des Domänencontrollers fungiert. Er speichert eine Kopie von Active Directory des Domänencontrollers. Hierzu findet in regelmäßigen Abständen eine Synchronisation zwischen beiden Rechnern statt. Fällt der Domänencontroller aus, so tritt BDC an seine Stelle.
BDC sollte eine Kopie von jedem am Domänencontroller vorhandenen Dienste besitzen.

Windows Scripting Host

Skriptsprachen sind Sprachen,

- die gegenüber einer herkömmlichen Programmiersprache einen eingeschränktem Befehlsumfang besitzen und
- mit der Probleme aus einem bestimmten Anwendungsfeld gelöst werden können.

Beispiele hierfür sind JavaSkript, VBScript oder Jscript. Z. B. wird JavaSkript eingesetzt um clientseitig Interaktionen zwischen Benutzer und Browser zu unterstützen. Der Befehlsumfang ist eingeschränkt, da z. B. keine Operation zum Schreiben von Daten auf die Festplatte existiert.

Der Windows Scripting Host ist eine Windows-Komponente, die Skripts lesen und ausführen kann. Dabei kann der Scripting Host mit unterschiedlichen Skriptsprachen umgehen, z. B. VBScript und JScript.

Durch Scripts können administrative Standardaufgaben automatisiert werden.

Beispiele:

- Bei der Abmeldung des Benutzers soll der Papierkorb geleert werden,
- Bei Rechnerstart sollen alle Benutzer über einen bestimmten Sachverhalt informiert werden (z. B. Meldung: ASW hat keinen Systembetreuer...)