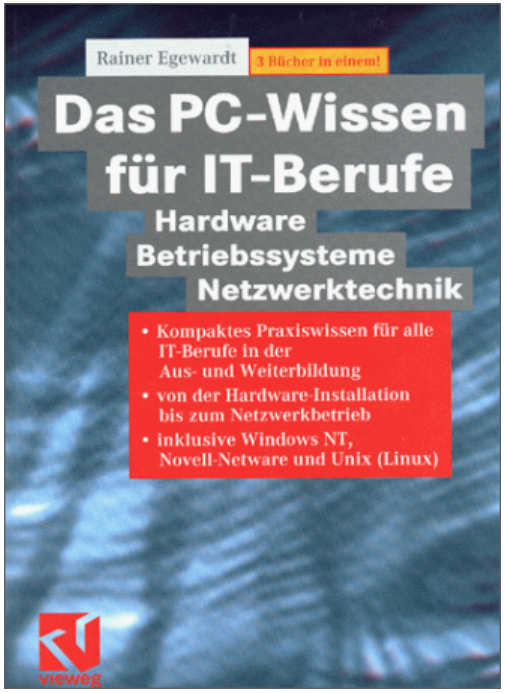
Auszug aus unserem Bestseller

Kapitel:
Windows 2000 Server

Autor: Rainer Egewardt



1. Auflage 600 Seiten

2. Auflage 1200 Seiten

Kompaktes Hardware-Wissen rund um Windows 2000 Server als Netzwerk-Betriebssystem

Stand 2002

Unsere Bücher „Das PC-Wissen für IT-Berufe" als Print-Medien, sind zu Bestsellern im IT-Buchmarkt geworden.

Powered by

PCT Solutions

„Das PC-Wissen für IT-Berufe“ ist in den nebenstehenden einzelnen Kapiteln als Download verfügbar

PCT-Solutions

info@pct-solutions.de
www.pct-solutions.de

Überblick über die weiteren Kapitel

- Micro-Prozessor-Technik
- Funktion von einzelnen Komponenten im PC
- Installation von einzelnen Komponenten im PC
- Netzwerk-Technik
- DOS
- Windows NT4 Server
- Windows 2000 Server
- Novell Netware Server
- Unix (Linux) Server

Bei allen Kapiteln handelt es sich um die Original-Verlags-Dateien, die zuletzt 2002 als Print-Medium veröffentlicht wurden.

Das nachfolgende Kapitel wurde auf der Basis von fundierten Ausbildungen, Weiterbildungen und umfangreichen Praxixerfahrungen erstellt und vom Verlag lektoriert. Für Schäden aus unvollständigen oder fehlerhaften Informationen übernehmen wir jedoch keinerlei Haftung.

IT-Lösungen • Dokumentationen • Präsentationen

Top-aktuelle Ebooks als Download

Unsere top-aktuellen Neuveröffentlichungen als EBooks zum Download von unserer Web-Site

PCT-Solutions

info@pct-solutions.de
www.pct-solutions.de

- Computer-Netzwerke Teil 1	Netzwerk-Design (Netzwerk-Hardware)
- Computer-Netzwerke Teil 2	Konfiguration eines Windows-Server basierten Netzwerkes
- Computer-Netzwerke Teil 3	DNS-, WINS-, DHCP-Konfiguration
- Computer-Netzwerke Teil 4	Optimieren von Windows-Netzwerken
- Computer-Netzwerke Teil 5	Netzwerkanbindung von Windows-Clients
- Computer-Netzwerke Teil 6	Scripting-Host in IT-Netzwerken
- Computer-Netzwerke Teil 7	Projekt-Management in IT-Netzwerken
- Datenbank Teil 1	MS-SQL-Server als Datenbank-Backend
- Datenbank Teil 2	MS-Access als Datenbank-Frontend
- Datenbank Teil 3	SQL-Programmierung (Transact-SQL)
- Mailing Teil 1	MS-Exchange-Server als Mail-Server
- Mailing Teil 2	Outlook als Mail-Client
- Internet Teil 1	Internet-Information-Server als HTML-Server
- Internet Teil 2	MS-Frontpage zum Erstellen eines HTML-Pools
- Internet Teil 3	Internet-Browser
- Web-Programmierung Teil 1	HTML
- Web-Programmierung Teil 1	DHTML
- Web-Programmierung Teil 1	CSS
- Web-Programmierung Teil 1	PHP
- Web-Programmierung Teil 1	JavaScript
- Web-Programmierung Teil 1	XML
- Software Teil 1	Professionelle Bildbearbeitung Corel PhotoPaint
- Software Teil 2	Professionelle Layouts mit Adobe Illustrator
- Software Teil 3	Grafisches Allerlei mit MS-Visio

und viele weitere EBooks zum Download auf unserer Internetseite

Hier sind Benutzereinstellungen immer verfügbar, egal von welchem Rechner im Netz man sich angemeldet. Für diese Funktion werden

- Active Directory
- Gruppenrichtlinie
- Offlinedateien
- Servergespeicherte Benutzerprofile

eingesetzt.

Remoteinstallationsdienste

Remoteinstallationsdienste ermöglichen das Installieren von Win2000-Pro-Computern über das Netzwerk. Dazu liegt eine lokale Installation des Betriebssystems auf dem Server, in Form einer Image-Datei, die zuvor erstellt und auf dem Server abgelegt wurde. Der Client wird beim ersten Booten dann über eine Startdiskette mit dem Server verbunden, und bekommt sein Betriebssystem vom Server installiert. Für diese Funktion werden

- Active Directory
- Gruppenrichtlinie
- Remoteinstallationsdienste

eingesetzt.

3.5.14 Benutzer-Verwaltung

Benutzer-, Computerkonten und Gruppen werden unter AD als Sicherheitsprincipals bezeichnet. Sicherheitsprincipals entsprechen Directory-Objekten, die eine Sicherheitskennung besitzen. Über die Sicherheitskennungen werden diese Objekte am Netzwerk angemeldet und können auf Ressourcen zugreifen. In AD-Computer und -Benutzer werden diese Objekte hinzugefügt.

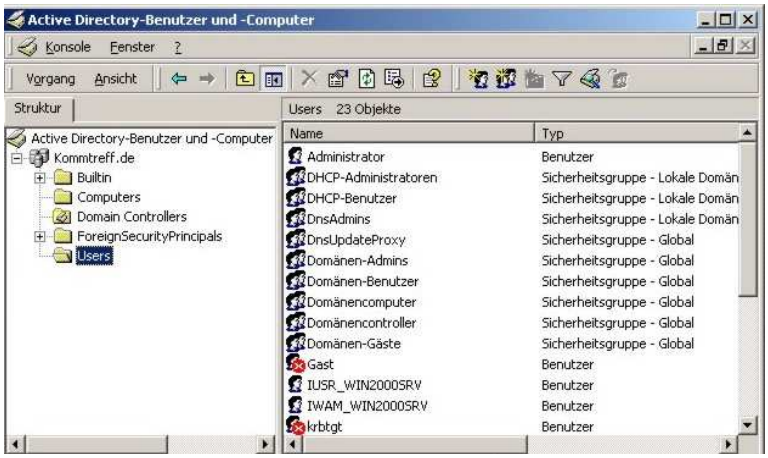


Abb. 156

Gibt es eine Vertrauensstellung zwischen einer Win2000-Domäne und einer Domäne außerhalb der eigenen Struktur, bekommen die Sicherheitsprincipals der fremden Domäne Zugriffsrechte auf die Ressourcen der eigenen Domäne, die als FREMDER SICHERHEITSPRINCIPAL der externen Domäne hinzugefügt werden. Diese können dann in lokalen Gruppen der externen Domänen aufgenommen werden. Zum Anzeigen dieser Objekte müssen unter AD-Benutzer- und -Computer die erweiterten Eigenschaften angezeigt werden.

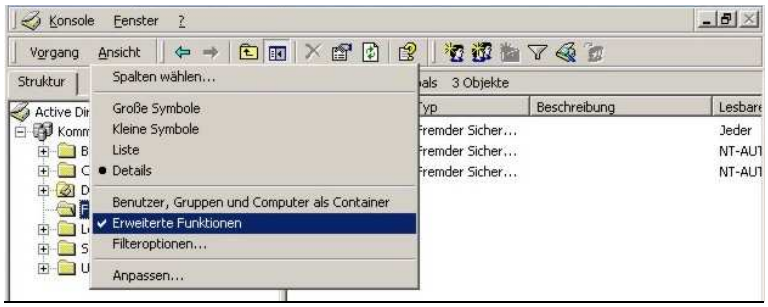


Abb. 157

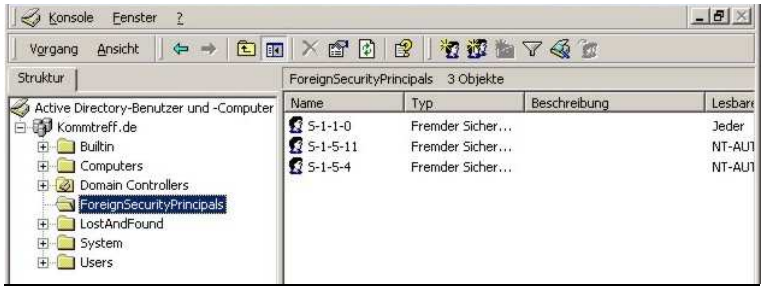


Abb. 158

Einrichten von Benutzern und deren Eigenschaften:

Start | Programme | Verwaltung | AD-Benutzer- und -Computer.

Benutzerkonten dienen der Authentifizierung eines Benutzers im Netzwerk.

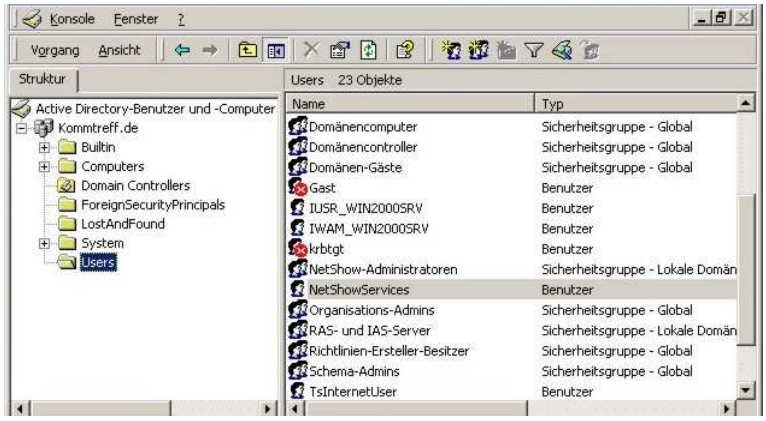


Abb. 159

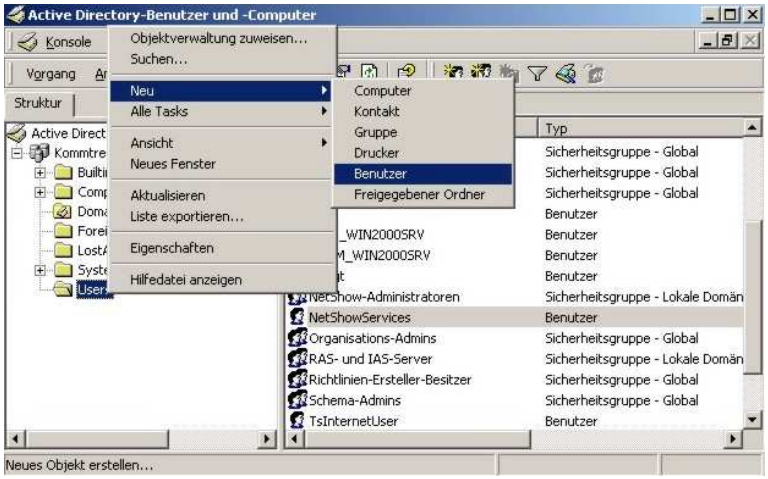


Abb. 160

Eigenschaften von Benutzerkonten werden unter Start | Programme | Verwaltung | AD-Benutzer- und -Computer | Verzeichnis Users auswählen | rechte Maustaste über den Benutzer | Eigenschaften | bearbeitet.

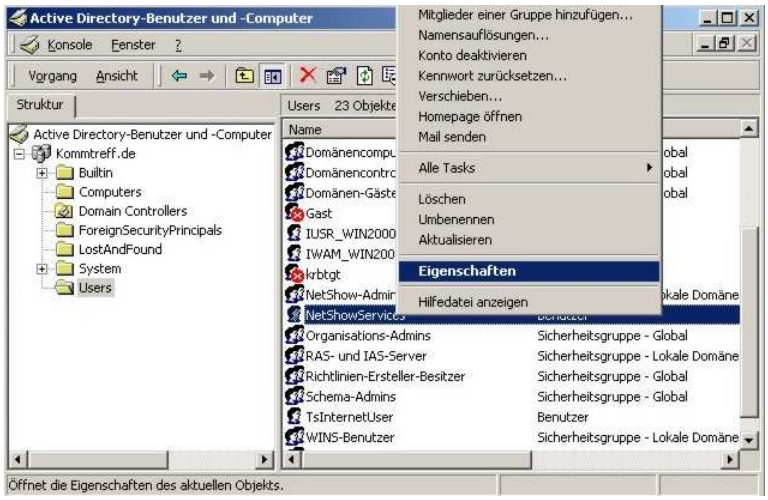


Abb. 161

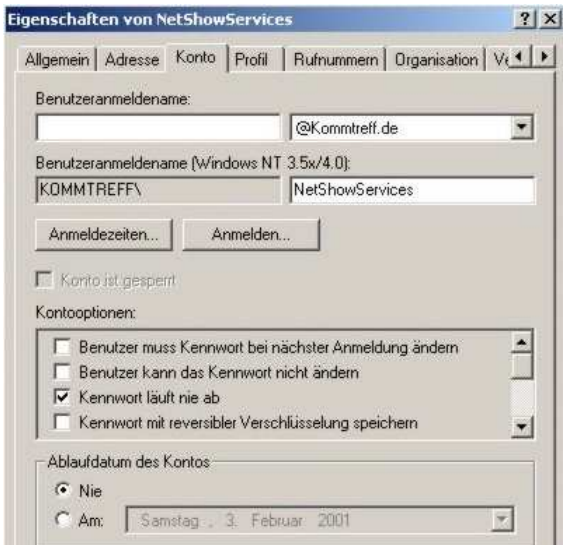


Abb. 162

Gruppen:

In Gruppen können Benutzer, andere Gruppen und Computer enthalten sein. Sie sind Objekte, die auf lokalen Computern sowie in AD vorhanden sind. Gruppen werden für

- Zugriffe auf freigegebene Ressourcen
- Filtern von Gruppenrichtlinieneinstellungen
- Erstellen von E-Mail-Verteilerlisten

verwendet.

Gruppen unterscheiden sich in

- Sicherheitsgruppen
- Verteilergruppen

Sicherheitsgruppen

In Sicherheitsgruppen sind Benutzer, Computer und andere Gruppen enthalten. Berechtigungen für Ressourcen sollten nur an Sicherheitsgruppen verteilt werden.

Verteilergruppen

Verteilergruppen werden nur für e-mail-Verteilerlisten verwendet. So können e-mails an ganze Gruppen von Benutzern versendet werden, nämlich denen, die der Verteilerliste angehören.

Organisationseinheiten

Für die Zusammenfassung von Objekten innerhalb einer Domäne, gibt es die Organisationseinheiten.

Gruppenrichtlinienobjekte

Gruppenrichtlinienobjekte beziehen sich auf Standorte, Domänen oder Organisationseinheiten, können jedoch nicht auf Gruppen angewendet werden. Sie sind eine Gruppe von Einstellungen, die auf Benutzer oder Computer angewendet werden.

Einrichten von Gruppen:

Win2000 unterscheidet in

- lokale
- globale und
- universelle

Gruppen.

Lokale Gruppen

Lokale Gruppen können universelle-, globale Gruppen oder Benutzerkonten aus beliebigen Domänen enthalten (Win2000- oder Win NT-Domänen). Rechte für lokale Gruppen können nur innerhalb der eigenen Domäne zugewiesen werden. Sie können Sicherheits- oder Verteilergruppen sein. Berechtigungen an diese Gruppen können nur in der lokalen Domäne erteilt werden.

Globale Gruppen

Globale Gruppen können Mitglied von lokalen Gruppen der eigenen Domäne sowie auf Mitgliedsservern und damit verbundenen Workstations oder vertrauten Domänen sein. Sie können nur Benut-

zer der eigenen Domäne enthalten, in der sie eingerichtet wurden. Mit globalen Gruppen können Gruppen gebildet werden, die innerhalb und außerhalb der Domäne verfügbar sind. Berechtigungen an diese Gruppen können in jeder Domäne der Gesamtstruktur erteilt werden.

Universelle Gruppen

Mitglieder von universellen Gruppen können aus jeder beliebigen Domäne oder der Gesamtstruktur stammen. Sie können globale-, oder lokale Gruppen sowie Benutzerkonten enthalten. Sie können Mitglied von lokalen Gruppen einer Domäne oder von anderen universellen Gruppen sein, nicht aber von globalen Gruppen. Globale Gruppen werden im globalen Katalog angezeigt und sollten nur globale Gruppen enthalten. Sie können Sicherheits- oder Verteilergruppen sein, die an jeder Stelle in einer Domänenstruktur oder Gesamtstruktur verwendet werden können. Berechtigungen an diese Gruppen können in jeder Domäne oder Gesamtstruktur verteilt werden.

Sind mehrere Gesamtstrukturen vorhanden, können Benutzer, die nur in einer Gesamtstruktur definiert wurden, nicht einer Gruppe einer anderen Gesamtstruktur zugeordnet werden. Auch können keinen Gruppen einer Gesamtstruktur Berechtigungen einer anderen Gesamtstruktur zugeordnet werden.

Sicherheitsgruppen werden in Listen geführt (DACLs), die Berechtigungen für Ressourcen und Objekte definieren.

Verteilergruppen können verwendet werden, wenn keine Sicherheitsgründe für die Gruppe vorliegen.

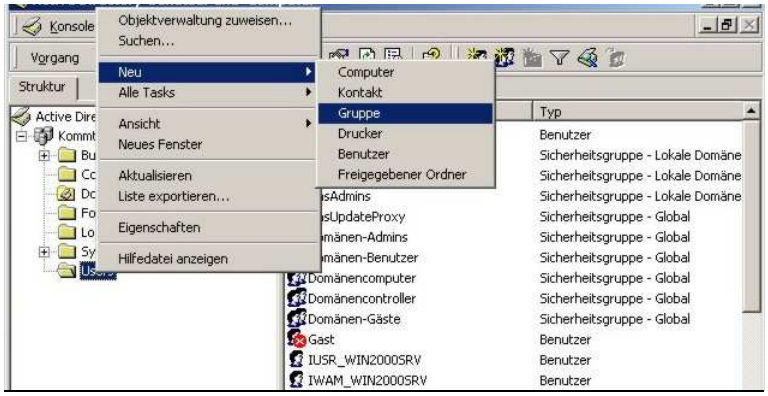


Abb. 163

Abb. 164

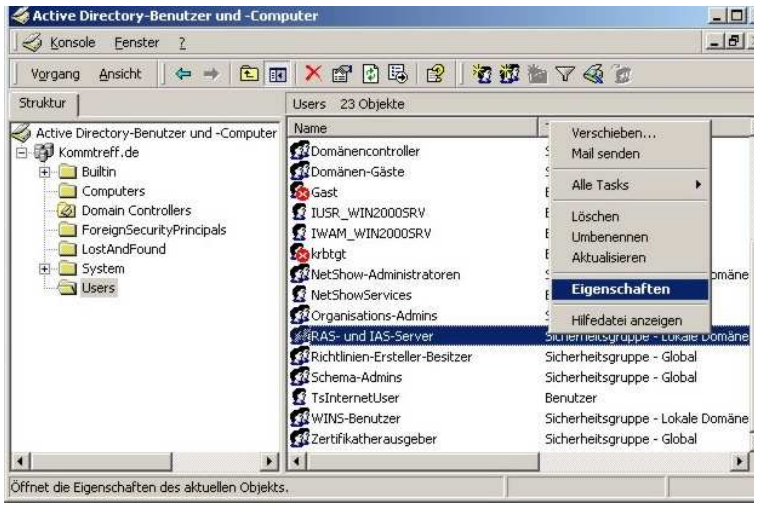


Abb. 165

Abb. 166

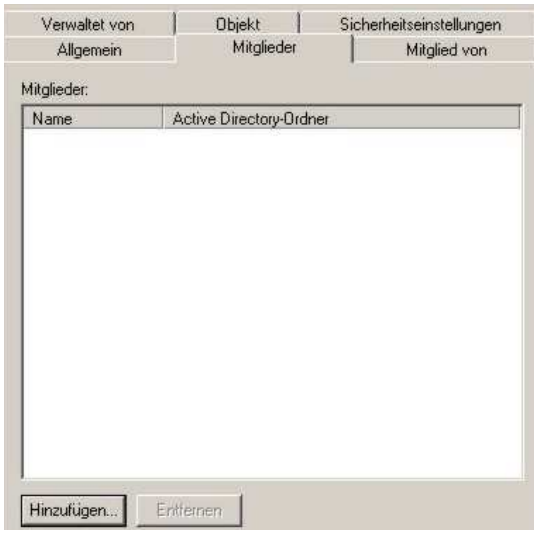


Abb. 167

Abb. 168

Abb. 169

Definition von Gruppen in Domänen

Werden Domänen im einheitlichen Modus ausgeführt (im Gegensatz zum gemischten Modus), können sie Konten, globale und universelle Gruppen aus allen vorhandenen Domänen enthalten. Es können in solchen Domänen jedoch keine Sicherheitsgruppen als universelle Gruppen erstellt werden. Gruppen können andere Gruppen enthalten, denen in jeder Domäne Berechtigungen zugeordnet werden können. Neu angelegte Gruppen werden als Sicherheitsgruppen im globalen Bereich definiert. Globale Gruppen können aber zu universellen Gruppen konvertiert werden, wenn die zu konvertierende Gruppe nicht einer anderen globalen Gruppe angehört.

Vordefinierte Gruppen:

Unter AD-Benutzer- und -Computer werden bei der Installation Standardgruppen installiert. Vordefinierte Gruppen in der lokalen Domäne werden im Verzeichnis VORDEFINIERT angelegt. Vordefinierte Gruppen im globalen Bereich werden unter BENUTZER angelegt. Unter dem Verzeichnis „Vordefiniert“ in AD werden folgende Gruppen angelegt:

- Konten-Operatoren
- Administratoren
- Sicherungs-Operatoren

- Gäste
- Druck-Operatoren
- Replikations-Operatoren
- Server-Operatoren
- Benutzer

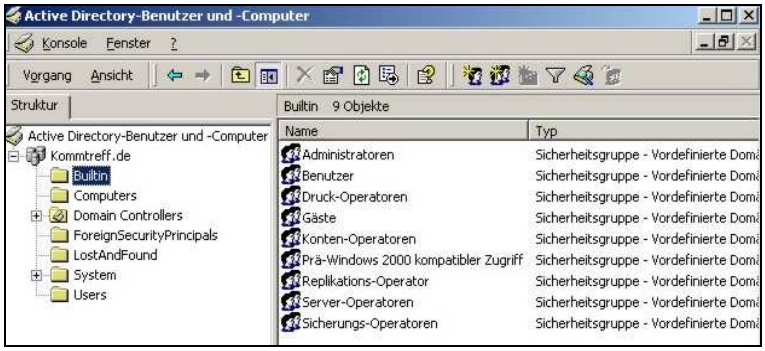


Abb. 170

Diese vordefinierten Gruppen verfügen über folgende vordefinierte Rechte:

Benutzerrecht	Gruppen, die standardmäßig über dieses Recht verfügen
Auf diesen Computer vom Netzwerk zugreifen	Administratoren, Jeder, Hauptbenutzer
Dateien und Dateiordner sichern	Administratoren, Sicherungs-Operatoren
Wechselprüfung umgehen	Jeder
Systemzeit ändern	Administratoren, Hauptbenutzer
Auslagerungsdatei erstellen	Administratoren
Programme debuggen	Administratoren
Herunterfahren von	Administratoren

einem Remotesystem aus	
Zeitplanungspriorität anhalten	Administratoren, Hauptbenutzer
Gerätetreiber laden und entfernen	Administratoren
Lokale Anmeldung	Administratoren, Sicherungs-Operatoren, Jeder, Gäste, Hauptbenutzer und Benutzer
Überwachungs- und Sicherheitsprotokoll verwalten	Administratoren
Firmwareumgebungsvariablen verändern	Administratoren
Einzelprozessprofil erstellen	Administratoren, Hauptbenutzer
Systemleistungsprofil erstellen	Administratoren
Dateien und Dateiordner wiederherstellen	Administratoren, Sicherungs-Operatoren
System herunterfahren	Administratoren, Sicherungs-Operatoren, Jeder, Hauptbenutzer und Benutzer
Besitz von Dateien oder anderen Objekten übernehmen	Administratoren

Unter „Benutzer“ werden folgende Gruppen angelegt:

- Zertifikatsherausgeber
- Domänen-Benutzer
- Domänen-Admins
- Organisations-Admins
- Domänencomputer
- Gruppenrichtlinien-Admins

- Domänencontroller
- Schema-Admins
- Domänen-Gäste

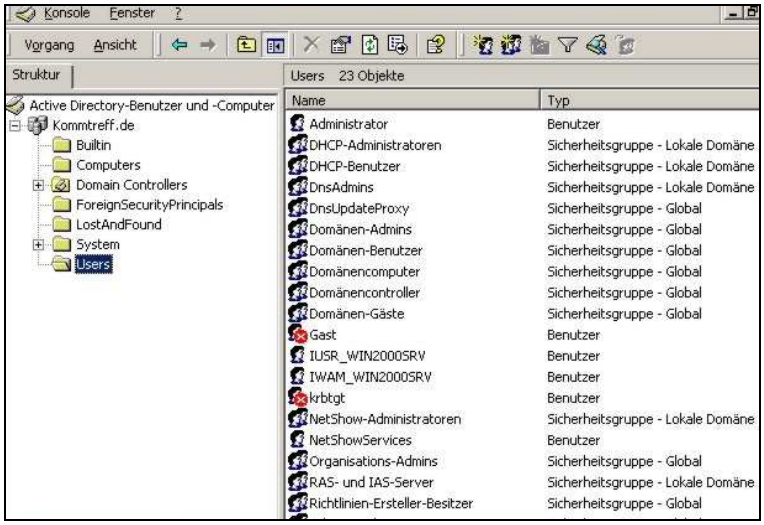


Abb. 171

Jedes erstellte Benutzerkonto in der Domäne wird aut. Mitglied in der Gruppe Domänen-Benutzer. Jedes erstellte Computerkonto in der Domäne wird aut. Mitglied der Gruppe Domänen-computer. Die Gruppe Domänen-Benutzer wird aut. Mitglied der Gruppe Benutzer. Die Gruppe Domänen-Admins wird aut. Mitglied der Gruppe Administratoren. Die Gruppe Domänen-Gäste wird aut. Mitglied der Gruppe Gäste in der selben Domänen.

Als Sondergruppen werden folgende Gruppen definiert:

Jeder	Jeder, der sich am Netzwerk anmeldet
Netzwerk	Benutzer, die auf Ressourcen über das Netzwerk zugreifen.
Interaktiv	Jeder am lokalen Computer angemeldete Benutzer, der auf eine lokale Ressource zugreift.

Mitgliedschaften in diesen Gruppen können nicht angezeigt oder manuell verändert werden. Universelle und verschachtelte Gruppen sowie getrennte Sicherheits- bzw. Verteilergruppen sind nur auf AD-Domänen-Controllern bzw. auf Mitgliedsservern verfügbar. Gruppenkonten auf eigenständigen Servern bzw. Win2000-Pro oder Win2000-Servern werden wie unter Win NT4 behandelt. Auf diesen Computern können nur lokale Gruppen erstellt, und diesen nur lokale Berechtigungen zugewiesen werden.

Werden Gruppen in andere Gruppen eingefügt, wird die Gruppenverwaltung vereinheitlicht. Die Optionen, wie Gruppen anderen Gruppen hinzugefügt werden können, bestimmt der einheitliche bzw. der gemischte Modus, in dem die Domäne läuft.

Gruppen in Domänen im einheitlichen Modus:

Universelle Gruppen können Konten, Computerkonten, andere universelle Gruppen oder globale Gruppen einer beliebigen Domäne enthalten.

Globale Gruppen können Konten derselben Domäne und andere globale Gruppen aus derselben Domäne enthalten.

Lokale Gruppen können Konten, globale und universelle Gruppen einer beliebigen Domäne enthalten.

Gruppen in Domänen im gemischten Modus:

Globale Gruppen können nur Konten enthalten. Lokale Gruppen können nur globale Gruppen und Konten enthalten. Universelle Gruppen werden nur in Win2000-Domänen unterstützt, die im einheitlichen Modus arbeiten (siehe Tabelle auf der nächsten Seite).

Zugriffssteuerung:

Die Zuweisung von Rechten und Berechtigungen in der Hierarchie von Containern, Gruppen, Benut-

zern, Computern und anderen Ressourcenobjekten wird durch eine verteilte Sicherheit vereinfacht. Dabei sollten, wie unter NT4, Benutzerrechte nur auf Gruppenebene zugewiesen werden. Wegen des Prinzips der Vererbung sollten Rechte so weit wie möglich oben in der Container-Struktur vergeben werden. Jeder Container kann dann speziellen Administratoren zur Verwaltung übertragen werden.

Domänen im einheitlichen Modus	Domänen im gemischten Modus
Sicherheits- und Verteilergruppen können über den Bereich „Universal“ verfügen.	Nur Verteilergruppen können über den Bereich „Universal“ verfügen.
Gruppen können unendlich verschachtelt werden.	Bei Sicherheitsgruppen ist die Verschachtelung auf Gruppen des Bereichs „Lokale Domäne“ beschränkt, deren Mitglieder Gruppen des Bereichs „Global“ sind (Windows NT 4.0-Regel). Verteilergruppen können unendlich verschachtelt werden.
Sicherheits- und Verteilergruppen können in den jeweils anderen Gruppentyp konvertiert werden. Gruppen mit den Bereichen „Global“ oder „Lokale Domäne“ können in den Gruppenbereich „Universal“ konvertiert werden.	Es sind keine Gruppenkonvertierungen zulässig.

Überwachung:

Nachstehende Überwachungen sollten zur Minimierung eines Sicherheitsrisikos durchgeführt werden:

- Fehlversuchsüberwachung bei An- bzw. Abmeldung,
- Erfolgsüberwachung bei An- und Abmeldung,
- Erfolgsüberwachung von Benutzerrechten,
- Benutzer- und Gruppenverwaltung,
- Änderungen der Sicherheitsrichtlinien,
- Neustarts,
- Herunterfahren des Systems,
- Erfolg- und Fehlversuchsüberwachung bei Datei- und Objektzugriffen,
- Erfolg- und Fehlversuchsüberwachung des Datei-Managers bei Lese-/Schreibzugriffen auf wichtige Dateien durch verdächtige Benutzer oder Gruppen,
- unzulässiger Zugriff auf wichtige Dateien,
- Erfolg- und Fehlversuchsüberwachung bei Dateizugriffen durch Drucker und Objektzugriffereignissen,
- Erfolg- und Fehlversuchsüberwachung des Druck-Managers bei Druckzugriffen durch verdächtige Benutzer oder Gruppen,
- unzulässiger Zugriff auf Drucker,
- Erfolg- und Fehlversuchsüberwachung bei Schreibzugriffen auf Programmdateien,
- Erfolg- und Fehlversuchsüberwachung für die Prozessverfolgung.

Verschlüsselung von Daten (siehe Abschnitt 3.5.17):

Dateien und Ordner können

- nur auf NTFS-Datenträgern verschlüsselt werden,

- nur von dem Benutzer geöffnet werden, der sie verschlüsselt hat,
- von Benutzern nicht freigegeben werden,
- beim Kopieren auf FAT-Partitionen ihre Verschlüsselung verlieren,
- über KOPIEREN und EINFÜGEN in einen verschlüsselten Ordner verschoben werden, damit die Verschlüsselung erhalten bleibt (nicht über DRAG&DROP),
- wenn sie komprimiert sind, nicht verschlüsselt werden,
- können aber von Benutzern, mit der Berechtigung zum Löschen von Datenobjekten, jederzeit gelöscht werden,
- können von Benutzern auf Remote-Computern ver-/entschlüsselt werden, wenn die Remote-Verschlüsselung freigegeben wurde.

Sicherheitsvorlagen:

Organisationseinheiten, die nur Benutzer enthalten, bekommen ihre Kontorichtlinien immer von einer Domäne. Deswegen sollten Kontenrichtlinien nicht für Organisationeinheiten ohne Computer konfiguriert werden. Dabei lässt Win2000 nur eine Kontorichtlinie zu, nämlich die der Stammdomäne der Domänenstruktur. Sind Win2000-Pro-Computer Mitglieder einer Win2000-Domäne, haben die Konto- und Kennwortrichtlinien Vorrang vor der lokalen Richtlinie für Domänencontroller, Server und Arbeitsstationen in der Domäne.

Werden Sicherheitseinstellungen in ein Gruppenrichtlinienobjekt in Active Directory importiert, gelten die lokalen Benutzereinstellungen für die Computerkonten nicht mehr. Gruppen und Benutzer werden aus den angegebenen Gruppen entfernt, wenn sie nicht in eingeschränkten Gruppen angegeben sind. D. h., die Option EINGESCHRÄNKTE GRUPPE sollte besser nur auf das Konfigurieren von lokalen Gruppen auf WS’s und Mitgliedsservern angewendet werden.

Werden Sicherheitsvorlagen in ein Gruppenrichtlinienobjekt importiert, erhalten aut. alle Konten, denen das Gruppenrichtlinienobjekt zugeordnet ist, die Sicherheitseinstellungen der Vorlage.

Datei- und Ordnerberechtigungen festlegen, anzeigen, ändern und entfernen:

Windows-Explorer | Datei oder Verzeichnis auswählen | rechte Maustaste über dem Objekt | Eigenschaften | Sicherheitseinstellungen.

Hier muss nun ein Benutzer/Gruppe ausgewählt bzw. über HINZUFÜGEN hinzugefügt werden. Sodann können unter BERECHTIGUNGEN Berechtigungen zugelassen bzw. verweigert werden.

Berechtigungen kann nur ändern, wer diese Berechtigung hat (vom Besitzer zugewiesen). Benutzer mit Vollzugriff können alle Dateien löschen. Werden Kontrollkästchen schattiert angezeigt, hat die Datei oder das Verzeichnis die Berechtigungen vom übergeordneten Verzeichnis geerbt (siehe Abb. 172).

Vererbung auf die Datei- und Ordnerberechtigungen:

Sind Berechtigungen für ein Verzeichnis erstellt worden, vererben sich diese Berechtigungen aut. an alle neu erstellten Verzeichnis bzw. Dateien in diesem Verzeichnis. Sollen keine Berechtigungen vererbt werden, muss NUR DIESEN ORDNER ÜBERNEHMEN FÜR aktiviert werden. Sollen bestimmte Verzeichnis/Dateien von der Vererbung ausgeschlossen werden, muss das Kästchen VERERBBARE ÜBERGEORDNETE BERECHTIGUNG ÜBERNEHMEN deaktiviert werden. Sind die Kontrollkästchen schattiert dargestellt, ist schon eine Vererbung eingetreten. Um die Vererbung zu ändern, kann der übergeordnete Ordner verändert werden, das Kontrollkästchen der übergeordneten Vererbung deaktiviert oder die gegensätzliche Be-

rechtigung

Abb. 172 Vergabe von Berechtigungen

ausgewählt werden. Ist für eine Berechtigung weder VERWEIGERN noch ZULASSEN ausgewählt, hat der Benutzer bzw. die Gruppe die Berechtigung durch eine Mitgliedschaft einer anderen Gruppe erhalten.

Besitzrecht an Dateien/Verzeichnis übernehmen:

Windows-Explorer | rechte Maustaste über dem Objekt | Eigenschaften | Sicherheitseinstellungen | Weitere | Besitzer.

Soll der Besitzer für alle untergeordneten Container und Objekte im Baum gleichzeitig geändert werden, muss das Kontrollkästchen BESITZER FÜR UNTERGEORDNETE CONTAINER UND OBJEKTE ERSETZEN aktiviert werden.

Ein aktueller Benutzer kann anderen Benutzern das Recht übertragen, den Besitz an dem Objekt zu übernehmen, so dass diese jederzeit dieses Recht ausüben können. Ein Administrator kann aber auch so jederzeit den Besitz an einem Objekt übernehmen, auch ohne, dass dies vorher vom Besitzer eingerichtet wurde.

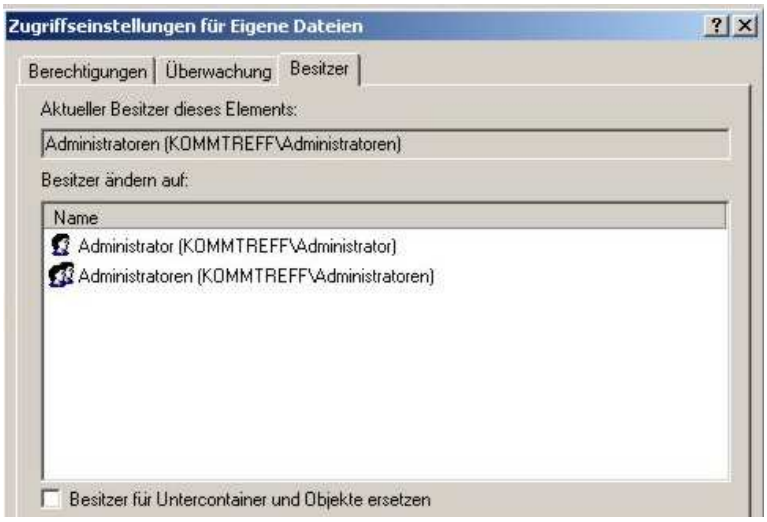


Abb. 173 Besitz an Dateien/Verzeichnis übernehmen

Überwachen von Dateien/Verzeichnissen:

Windows-Explorer | Datei oder Ordner | rechte Maustaste auf die Datei bzw. den Ordner | Eigenschaften | Sicherheitseinstellungen | Erweitert | Überwachung.

Unter HINZUFÜGEN kann jetzt ein Benutzer oder eine Gruppe ausgewählt werden, die überwacht werden soll. Um die Überwachung einer Gruppe oder eines Benutzers anzuzeigen, muss auf den Namen geklickt werden und dann auf ANZEIGEN/BEARBEITEN. Zum Entfernen einer Überwachung, auf ENTFERNEN klicken.

Achtung: Um Dateien/Verzeichnis zu überwachen, muss die Einstellung OBJEKTZUGRIFFSVERSUCHE ÜBERWACHEN in den