

# Inhaltsverzeichnis

<b>Vorwort</b>	<b>13</b>
<b>Einleitung</b>	<b>15</b>
<b>1 Einführung</b>	<b>19</b>
1.1 Unterschiedliche Aspekte der Sicherheit	19
<b>2 Die Architektur von Windows NT</b>	<b>23</b>
2.1 Systemübersicht	26
2.1.1 Client/Server-Modell	27
2.1.2 Objektmodell	30
2.1.3 Symmetrisches Multiprocessing	31
2.2 Die Module von Windows NT	32
2.3 Hardware Abstraction Layer (HAL)	35
2.4 Micro-Kernel	35
2.5 Prozessorzeitvergabe und Prioritäten	37
2.6 Symmetrisches Multiprocessing (SMP)	39
2.7 Micro-Kernel-Objekte	39
2.8 Dienste der Windows NT Executive	41
2.8.1 E/A-Manager	42
2.8.2 Objekt-Manager	47
2.8.3 Sicherheitsmodell für Windows NT	48
2.8.4 Prozeß-Manager	49
2.8.5 Lokaler Prozeduraufruf (LPC – Local Procedure Call)	50
2.8.6 VM-Manager	51
2.8.7 Fensterverwaltung	53
2.8.8 Graphics Device Interface (GDI)	53
2.8.9 Grafikgerätetreiber	54
2.8.10 Umgebungssysteme	54
2.9 Netzwerkfunktionen von Windows NT	57
2.9.1 Eingebaute Netzwerkkomponenten	60
2.9.2 Transport-Protokolle	64
2.10 Der Einsatz der Windows-NT-Netzwerkfunktionen	65
2.11 Remote Access Services (RAS)	69
<b>3 Das Sicherheitsmodell von Windows NT</b>	<b>73</b>
3.1 Merkmale des Sicherheitsmodells	74

3.2	Aufbau des Sicherheitsmodells	76
3.2.1	NetLogon-Dienst (Anmeldevorgänge)	83
3.2.2	NetLogon-Dienst (Domänen-Controller-Abgleich)	87
3.2.3	Objekte und Access Token	89
3.2.4	Auditing – Überwachen von Ereignissen	94
<b>4</b>	<b>Windows-NT-Server-Domänen</b>	<b>111</b>
4.1	Workgroup-Prinzip	111
4.1.1	Beglaubigungsvorgänge in einer Workgroup	115
4.2	Aufbau und Stuktur von Domänen	119
4.2.1	Synchronisationsparameter für die Domäne in der Registry	122
4.2.2	Synchronisation der Domäne über WAN-Verbindungen	127
4.2.3	Manuelle vollständige Synchronisation	129
4.2.4	Unterstützte Domänen-Clients	131
4.2.5	Domänen-Sicherheit durch SIDs	132
4.3	Vertrauensstellungen zwischen Domänen (Trust Relationships)	142
4.3.1	Trusting versus Trusted Domain	143
4.3.2	Vertrauensstellungstypen	144
4.3.3	Einsatz der Pass-Through-Beglaubigung	146
4.3.4	Einrichten von Vertrauensstellungen	149
4.4	Domänen-Modelle	152
4.4.1	Single-Domänen-Modell	153
4.4.2	Master-Domänen-Modell	155
4.4.3	Multiple-Master-Domänen-Modell	158
4.4.4	Complete-Trust-Modell	160
4.4.5	Nachteilige Eigenschaften der Domänen-Modelle	162
4.4.6	Synchronisation der Domänen-Datenbank	164
4.4.7	Einbindung von Windows NT Workstations in eine Domäne	165
<b>5</b>	<b>Benutzer-Accounts unter Windows NT</b>	<b>169</b>
5.1	Funktionen des Benutzermanagers für Domänen	171
5.2	Grundsätzliches zum Arbeiten mit dem Benutzermanager für Domänen	172
5.3	Einrichten neuer Benutzerkonten	178
5.4	Bearbeiten bestehender Benutzer-Accounts	182
5.5	Standard-Benutzer-Accounts	183
5.6	Account Policy	186

5.7	User Rights Policy	190
5.7.1	Standard-Benutzerrechte	194
5.7.2	Erweiterte Standard-Benutzerrechte	197
5.8	Verwaltungsmöglichkeiten für Benutzer-Accounts	200
5.8.1	Kopieren von Benutzer-Accounts	201
5.8.2	Löschen von Benutzer-Accounts	201
5.8.3	Benutzer finden, die bestimmter Gruppe angehören	202
5.8.4	Umbenennen von Benutzern	203
5.9	Sicherheitsrichtlinien	204
<b>6</b>	<b>Einsatz und Verwendung von Gruppen</b>	<b>207</b>
6.1	Globale Gruppen versus lokale Gruppen	208
6.2	Zugriffsberechtigung, Benutzerrecht und eingebaute Fähigkeiten	211
6.3	Standardgruppen und implizite Gruppen	215
6.4	Einrichten und Verwalten von Gruppen	226
6.4.1	Einrichten von globalen Gruppen	227
6.4.2	Einrichten lokaler Gruppen	228
6.4.3	Kopieren von Gruppen	232
<b>7</b>	<b>Verwaltung von Verzeichnisfreigaben</b>	<b>237</b>
7.1	Einrichten von Share-Verzeichnissen	239
7.2	Verwalten von Shares über Server-Manager	245
7.2.1	Löschen eines Computerkontos	247
7.2.2	Hinzufügen eines Computerkontos in eine Domäne	248
7.2.3	Properties anzeigen lassen	248
7.3	Anzeigen und Ändern von Shares	253
7.4	Windows NT Services starten und stoppen	255
7.5	Freigabeberechtigung und ACLs	256
7.6	Definition von Laufwerksbuchstaben	262
7.7	Datei- und Verzeichnisberechtigungen unter NTFS	265
7.7.1	Vergabe von Zugriffsberechtigungen für Verzeichnisse	270
7.7.2	Vergabe von Zugriffsberechtigungen für Dateien	276
7.8	Weitergabe von ACLs	282
7.8.1	Neu eingerichtete Dateien in einem Verzeichnis	282
7.8.2	Neu eingerichtete Verzeichnisse in einem Verzeichnis	284
7.8.3	Handhabung von Creator Owner, wenn Dateien neu eingerichtet werden	285

7.8.4	Handhabung von Creator Owner, wenn Verzeichnisse neu eingerichtet werden	287
7.8.5	Copy (Kopieren) und Move (Verschieben)	288
7.8.6	Attribute für Verzeichnisse und Dateien	289
7.8.7	Ändern der Zugriffsrechte auf Command-Ebene	290
<b>8</b>	<b>Benutzer-Profil und System-Policy</b>	<b>293</b>
8.1	Was ist ein Benutzer-Profil?	293
8.1.1	Lokales Profil	294
8.1.2	Serverbasierendes Profil	300
8.1.3	Arbeitsweise von Default-Profiles	302
8.1.4	Arbeitsweise vom System-Default-Profil	305
8.1.5	Lokale Speicherung von Roaming-Benutzer-Profiles	306
8.1.6	Einrichten eines neuen Benutzer-Profiles	309
8.1.7	Unterschiedliche Hardwarekonfigurationen	313
8.1.8	Anpassung des Default-Benutzer-Profiles für alle Computer in einer Domäne	313
8.1.9	Logon über Slow Network	314
8.2	System Policies unter Windows NT	316
8.2.1	Policy-Optionen	318
8.2.2	Policy-Einstellungen für Benutzer/Gruppen	323
8.2.3	Policy-Einstellungen für Workstations	327
8.3	Logon-Skripts	336
8.3.1	Automatisches Replizieren der Logon-Skripts	338
8.3.2	Home Directory eines Benutzers	339
<b>9</b>	<b>Replikationsdienste von Windows NT</b>	<b>341</b>
9.1	Einrichten der Replikationsdienste	344
9.2	Einrichten des Export-Servers	346
9.2.1	Replizierung von Logon-Skripts	347
9.3	Einrichten eines Import-Servers	348
<b>10</b>	<b>Verwaltung der Netzwerkdateien</b>	<b>351</b>
10.1	Windows-NT-Dateisysteme	351
10.1.1	Aufbau des FAT-Dateisystems unter Windows NT	353
10.1.2	Aufbau von NTFS unter Windows NT	354
10.1.3	Zugriffsberechtigung für Dateien und Verzeichnisse	358
10.1.4	Komprimierung und NTFS	359
10.2	Festplattenverwaltung – der Disk-Administrator	359
10.2.1	Konzepte zur Erhöhung der Sicherheit	361

10.3	Der Disk-Administrator unter Windows NT	365
10.3.1	Allgemeine Bemerkungen zur Bedienung des Disk-Administrators	366
10.3.2	Aufruf des Disk-Administrators	366
10.3.3	Erste Schritte im Disk-Administrator	368
10.3.4	Verändern der Eigenschaften eines Festplattenlaufwerks	371
10.3.5	Einrichten eines Mirror-Sets	374
10.3.6	Anlegen eines Volume-Sets	375
10.3.7	Anlegen eines Stripe-Sets ohne Parität	376
10.3.8	Definition eines Stripe-Sets mit Parität	376
10.4	Systemdiagnose, Recovery und Repair	378
10.4.1	Einstellung der System-Recovery-Optionen	379
10.4.2	Last Known Good Configuration	380
10.4.3	Repair-Prozeß	380
10.4.4	Beheben eines System-Boot-Fehlers	381
10.5	Resource Kit von Microsoft	384
10.5.1	Account- und Benutzer-Management	384
10.5.2	Server-Management	385
10.5.3	Datei- und Verzeichnis-Management	386
<b>11</b>	<b>Einsatz der Registry</b>	<b>387</b>
11.1	Starten des Registry-Editors	388
11.2	Bedeutung der Hauptschlüssel	389
11.3	Hives – Speicherort für Registry-Einträge	390
11.4	Fehlertoleranz in der Registry	391
11.4.1	HKEY_LOCAL_MACHINE	392
11.4.2	HKEY_CURRENT_USER	393
11.5	Struktur und Schlüssel der Einträge	395
11.6	Bearbeiten der Registry	398
11.6.1	Ändern und Hinzufügen von Einträgen	398
11.6.2	Suchen von Schlüsseln und Einträgen	399
11.7	Wie man die Registry schützt	401
11.7.1	Überwachen von Zugriffen auf die Registry	404
11.7.2	Pflege der Registry	406
11.7.3	Sicherung und Wiederherstellung der Registry	412
11.8	Praktischer Einsatz spezieller Änderungen	415
11.8.1	Erstellung einer individuellen Logon-Nachricht	415
11.8.2	Automatischen Logon einrichten	416
11.8.3	Ändern des Logon-Bildschirms	418

## *Inhaltsverzeichnis*

11.8.4 Herunterfahren ohne Logon	419
11.8.5 Aktivierung der Optionen Shutdown und Power Off	420
11.8.6 Anzeigen Last-Logged-In-Benutzer	421
11.8.7 Durchsuchen der AUTOEXEC.BAT	421
<b>Anhang A</b>	<b>423</b>
<b>Anhang B</b>	<b>441</b>
<b>Glossar</b>	<b>457</b>
<b>Stichwortverzeichnis</b>	<b>467</b>