

Errata zum Buch

Bernhard Tritsch:

Microsoft Windows NT 4.0 Terminal Server Edition einsetzen.

Microsoft Press 1999, ISBN 3-86063-499-2

Bei der ersten Druckauflage dieses Buches haben sich leider einige Druckfehler eingeschlichen, welche die Aussagekraft einiger Tabellen stark beeinträchtigen. Beiliegend finden Sie die richtige Darstellung.

Seite 19

RAM_{Minimum}	= 32 MB + (Benutzerzahl · 8 MB)
RAM_{Typisch}	= 64 MB + (Benutzerzahl · 16 MB)
$RAM_{\text{PowerUser}}$	= 64 MB + (Benutzerzahl · 32 MB)
Auslagerungsspeicher	= RAM · 2,5
Netzwerkbandbreite _{Minimum}	= Benutzerzahl · 10 KB/s
Netzwerkbandbreite _{Typisch}	= Benutzerzahl · 25 KB/s

Seite 26–29

Die einzelnen Standarddienste und ihre Funktionalitäten sollen im Folgenden aufgelistet werden. Benötigt ein Dienst einen anderen um starten zu können, so wird dies vermerkt. Die fett markierten Dienste sind für den Standardbetrieb von Windows NT im Netzwerk bzw. eines Windows Terminal Servers zwingend erforderlich.

- **Arbeitsstationsdienst:** Mit diesem Dienst können von einem Computer Verbindungen zu Netzwerkressourcen hergestellt und verwendet werden.
- **Client Service for NetWare:** Dieser Dienst ermöglicht einem System unter Windows NT den Zugriff auf Novell NetWare Netzwerke.
- **Ablagemappen-Server:** Dieser Dienst erlaubt das Ausschneiden und Einfügen über das Netzwerk.
- **Computer-Suchdienst:** Mit dem Computer-Suchdienst listet ein Computer all diejenigen Ressourcen auf, die er zur Verfügung stellen kann. Dazu gehören z.B. der Computername, freigegebene Verzeichnisse und Drucker. Zudem stellt ein einziger Computer im Netzwerk, auf dem der Computer-Suchdienst ausgeführt wird, allen anderen Clients die Liste aller im Netz verfügbaren NT-Ressourcen zur Verfügung (Browse-Master).
- **DHCP Client:** Mit Hilfe des DHCP-Client-Dienstes kann ein Netzwerk-Computer eine IP-Adresse von einem DHCP-Server erhalten. Dieser Dienst ist nur verfügbar, wenn das TCP/IP-Protokoll installiert wurde.
- **Druck-Server-Dienst für den Macintosh:** Dieser Dienst ermöglicht das Drucken von Macintosh-Computern aus und kann nur auf Computern unter Windows NT Server installiert werden.
- **Ereignisprotokollierdienst:** Mit diesem Dienst werden Ereignisse auf dem lokalen Computer aufgezeichnet. Bevor die protokollierten Ereignisse in der Ereignisanzeige angezeigt werden können, muss der Ereignisprotokollierdienst gestartet werden.
- **File Server for Macintosh (SFM-Datei-Server):** Dieser Dienst ermöglicht die gemeinsame Nutzung von Dateien mit Macintosh-Computern. Der Befehl steht nur auf Computern unter Windows NT Server zur Verfügung.
- **FTP-Veröffentlichungsdienst:** Dieser Dienst ist nur verfügbar, wenn der Internet Information Server installiert wurde.
- **Gateway Service for NetWare:** Dieser Dienst erlaubt es einem NT Server, auf Ressourcen in einem Novell-NetWare-Netzwerk zuzugreifen. Zudem können mit Hilfe des Gateway-Services diese Ressourcen anderen Computern ohne direkten Novell-Zugriff wiederum per Microsoft Netzwerkabbindung transparent zur Verfügung gestellt werden.

- *TCP/IP-Druck-Server*: Der TCP/IP-Druck-Server-Dienst ist die Implementation des unter Unix bekannten LPD-Druckdienstes. Dieser Dienst ist nur verfügbar, wenn das TCP/IP-Protokoll installiert wurde.
- *Plug & Play*: Ein zusätzlich installierbarer Dienst, der die automatische Konfiguration von ISA Plug&Play-Geräten unterstützt.
- *Microsoft DHCP Server*: Dieser Dienst ist nur auf Windows NT Server-Computern verfügbar, auf denen das TCP/IP-Protokoll und der DHCP-Server installiert wurden. Der Microsoft DHCP-Server-Dienst stellt IP-Adressen für Netzwerk-Clients bereit.
- *Nachrichtendienst*: Mit diesem Dienst können an einem Computer Nachrichten empfangen werden. Die einem Computer zugewiesenen Namen werden beim Senden der Nachricht zur Identifikation verwendet.
- *NetLogon (Anmeldedienst)*: Der Anmeldedienst überprüft Anmeldeanfragen und steuert die Replikation der Benutzerkontendatenbank in einer Domäne. Dieser Dienst muss auf allen Servern einer Domäne gestartet sein, die als Anmeldeserver in einem Netzwerk verwendet werden sollen. Durch die Deaktivierung dieses Dienstes kann z.B. vermieden werden, dass in einem Netzwerk mit vielen Servern die Replikation von Benutzerdatenbankinformation das Netzwerk zu stark belastet. Allerdings werden dann Anmeldungen von Client-Computern eben auch nur noch von denjenigen Servern angenommen, die den NetLogon-Dienst aktiviert haben.
- *Network DDE*: Unterstützung von Dynamic Data Exchange über das Netzwerk, z.B. für verteilte Clipboards.
- *Netzwerkmonitoragenten*: Der Netzwerkmonitoragent unterstützt die entfernte Überwachung der Netzwerkkommunikation eines Clients.
- *NT-LM-Sicherheitsdienst*: Dieser Dienst ist nur verfügbar, wenn der NT-LanManager-Sicherheitsdienst installiert wurde. Er ermöglicht die Integration von älteren, LanManager-basierten Servern in ein NT-Server-Netzwerk.
- *Remoteboot*: Dieser Dienst ermöglicht es den Computern im Netzwerk, ihr Betriebssystem vom Computer herunter zu laden. Der Dienst steht nur auf Computern unter Windows NT Server zur Verfügung und setzt spezielle Hardware voraus (Boot-PROMs auf den Netzwerkkarten der Clients).
- *RAS-Verbindungs-Manager*: Dieser Dienst ist nur verfügbar, wenn der RAS-Dienst installiert wurde. Er verwaltet den Aufbau und den Betrieb von RAS-Verbindungen (Remote Access).
- *Remote Access ISNSAP Service*: Dieser Dienst ist nur verfügbar, wenn der RAS-Dienst installiert wurde.
- *Remote Access Server*: Dieser Dienst ist nur verfügbar, wenn der RAS-Dienst installiert wurde.
- *Remote Procedure Call (RPC) Locator*: Bei diesem Dienst handelt es sich um den RPC-Namensdienst für Microsoft Windows NT. Der RPC-Locator wird genutzt, um verteilten Anwendungen die Verwendung des Microsoft RPC-Namensdienstes zu ermöglichen. Der RPC-Locator verwaltet die RPC-Namensdienstdatenbank. Eine verteilte Anwendung auf einem Server kann sich mit Hilfe des RPC-Locator als verfügbar registrieren lassen. Eine verteilte Anwendung auf einem Client kann mit Hilfe des RPC-Locator nach verfügbaren kompatiblen Serveranwendungen suchen.
- *Remote Procedure Call (RPC) Service*: Der Remote Procedure Call (RPC)-Dienst ist das RPC-Teilsystem für Microsoft Windows NT. Das RPC-Teilsystem enthält die Endpunktzurordnung und verschiedene andere RPC-Funktionen. Der RPC-Dienst verwaltet die Datenbank der Endpunktzurordnung. Eine verteilte Anwendung auf einem Server kann mit Hilfe des RPC-Locator ihre Endpunkte registrieren lassen. Eine verteilte Anwendung auf einem Client kann über die Client Run-Time Library den Remote Procedure Call (RPC)-Dienst nach Informationen über die Endpunkte abfragen. UNIX-RPCs sind leider nicht kompatibel mit den NT-RPCs.
- *Server-Dienst*: Mit diesem Dienst kann ein Computer Ressourcen im Netzwerk freigeben und an einen ausreichend autorisierten Client Systeminformationen weitergeben.
- *Simple TCP/IP Services*: Dieser Dienst ist nur verfügbar, wenn TCP/IP und die einfachen TCP/IP-Dienste installiert wurden. Die einfachen TCP/IP-Dienste unterstützen die TCP/IP-Dienste Character Generator (Zeichengenerator), Daytime, Discard, Echo und Quote of the Day (Tagesquote).

Sind diese gestartet, kann der Computer auf Anfragen anderer Computer antworten, die diese Protokolle unterstützen.

- **SNMP:** Mit diesem Dienst kann ein Server seinen aktuellen Status an ein SNMP-Verwaltungssystem im TCP/IP-Netzwerk melden. Dieser Befehl ist nur verfügbar, wenn TCP/IP und SNMP installiert wurden.
- **Spooler:** Dieser Dienst verwaltet die Zwischenspeicherungsdateien für Drucker.
- **TCP/IP NetBIOS Helper:** Dieser Dienst ist nur verfügbar, wenn TCP/IP installiert wurde, und erlaubt die Verwendung von NetBIOS-Funktionalitäten über TCP/IP.
- **USV:** Zur Konfiguration dieses Diensts muss das Symbol USV (Unterbrechungsfreie Stromversorgung) in der Systemsteuerung verwendet werden. Wenn der USV-Dienst so konfiguriert wurde, dass im Moment des Herunterfahrens ein Befehl ausgeführt werden soll, so muss dieser Befehl innerhalb von 30 Sekunden ausgeführt sein. Andernfalls ist das sichere Herunterfahren des Computers gefährdet.
- **Verzeichnisreplikationsdienst:** Dieser Dienst kopiert ausgewählte Dateien auf bestimmte Server.
- **Warndienst:** Mit diesem Dienst können Warnmeldungen an bestimmte Benutzer oder an alle mit dem Server verbundenen Benutzer verschickt werden. Die Warnmeldungen beziehen sich auf Sicherheits- und Zugriffsprobleme sowie Probleme bei Benutzersitzungen. Mit dem Server-Manager werden die Benutzer und Computer festgelegt, die Admin-Warnmeldungen erhalten sollen. Die Warnmeldungen werden als Windows NT-Meldungen vom Server an die einzelnen Computer gesendet. Damit ein Benutzer Warnmeldungen empfangen kann, muss auf dem Computer des Benutzers der Nachrichtendienst (Messenger) ausgeführt sein.
- **Windows Internet Name Service:** Dieser Dienst ist nur unter Windows NT Server verfügbar, wenn TCP/IP und WINS installiert wurden. Der WINS-Dienst führt die Zuordnung von Microsoft Computernamen zu IP-Adressen für Client-Computer in einem Netzwerk durch.
- **Zeitplandienst:** Mit diesem Dienst kann ein Computer Programme mit dem Befehl *at* zu einem bestimmten Zeitpunkt starten. Der Zeitplandienst ist standardmäßig so konfiguriert, dass er im Systemkonto des lokalen Computers ausgeführt wird. Wenn der Zeitplandienst dieses Konto benutzt, gibt es keine Einschränkungen bezüglich der Aufträge, die mit dem Zeitplandienst gestartet werden können. Diese Aufträge verfügen jedoch nur über eingeschränkten Netzwerkzugriff, da das Systemkonto eines lokalen Computers von anderen Computern nicht erkannt wird. Um diese Einschränkungen bezüglich des Netzwerkzugriffs zu überwinden, können Sie den Zeitplandienst so konfigurieren, dass er in einem Benutzerkonto ausgeführt wird. So gilt für Aufträge, die mit dem Zeitplandienst gestartet werden, der Netzwerkzugriff des Benutzerkontos. Da in diesem Fall der Zeitplandienst das lokale Systemkonto nicht verwendet, können nur Anwendungen gestartet werden, die kein Fenster benötigen. Um den Zeitplandienst so zu konfigurieren, dass er in einem Benutzerkonto ausgeführt wird, muss der Benutzer-Manager verwendet werden, um diesem Benutzerkonto auf einem lokalen Computer das Recht *Anmelden als Dienst* zu erteilen. Dann wird in der Systemsteuerung das Symbol *Dienste* ausgewählt um den Zeitplandienst zu konfigurieren. Dies geschieht, indem auf *Startart* geklickt und unter *Anmelden als* die Option *Dieses Konto* gewählt wird.

Ein Windows Terminal Server besitzt darüber hinaus noch weitere Systemdienste, die im Folgenden aufgeführt werden.

- **Terminal Server:** Dieser Dienst realisiert die zentralen Bestandteile zur Erweiterung von Windows NT für die interaktive Benutzung von mehreren Anwendern.
- **Terminal Server-Lizensierungsdienst:** Überwachen der genutzten WTS-Lizenzen.



Seite 34

Option	Verbindungsspezifische Einstellungen	Benutzerspezifische Einstellungen	Clientspezifische Einstellungen
TCP/IP-Protokoll	●	○	○
Konfiguration der verwendeten LAN-Adapter	●	○	○
Zähler für maximale Verbindungen	●	○	○
Protokollierung	●	○	○
Zeitlimits für Verbindungen	●	●	○
Zeitlimits für getrennte Verbindungen	●	●	○
Zeitlimit für Leerlauf	●	●	○
Sicherheit (Verschlüsselung)	●	○	○
Automatisches Anmelden	●	●	●
Initiales Programm	●	●	●
Überschreiben von Benutzerprofilen	●	○	○
Behandlung unterbrochener Verbindungen	●	●	○
Automatische Wiederaufnahme von Verbindungen	●	●	○
Anbindung von Client-Geräten	●	●	○

Table 2.1: Konfigurationseinstellungen über die Terminal Server Verbindungskonfiguration, den Benutzer-Manager oder den Client

Seite 49

Recht	Kein Zugriff	Gäitezugriff	Benutzerzugriff	Volle Kontrolle
Informationen über die Sitzung abfragen	○	○	●	●
Informations- bzw. Verbindungsparameter einstellen	○	○	○	●
Zurücksetzen von Sitzungen	○	○	○	●
Am Server anmelden	○	●	●	●
Sitzungen abmelden	○	○	○	●
Nachrichten senden	○	○	●	●
Zu getrennten Sitzungen verbinden	○	○	●	●
Trennen einer Sitzung	○	○	○	●

Table 2.4: Zugriffsrechte einer WTS-Verbindung

Seite 50

Karteikarte	Domäne	Server	Sitzung
Benutzer	●	●	○
Sitzungen	●	●	○
Prozesse	●	●	●
Informationen	○	●	●

Table 2.5: Angezeigte Karteikarten mit Informationen in der Terminal Server-Verwaltung in Abhängigkeit des gewählten Objekts Domäne, Server oder Sitzungen

Seite 55

Werkzeug	Modifikation	Entfernt ausführbar
Benutzer-Manager	Terminal Server-Basisverzeichnis und Terminal Server-Profilpfad als zusätzliche Eigenschaften im Umgebungsprofil für Benutzer. Spezielles Dialogfenster für die Konfiguration von Benutzersitzungen	●
Task-Manager	Benutzerzuordnung wird in der Karteikarte <i>Prozesse</i> angezeigt	○
Systemsteuerung	Zusätzliche WTS-Dienste, WTS-Geräte und ODBC-Datenquellen	○
Systemmonitor	Zusätzliche Objekte zur Überwachung eines Terminal Servers	●
Ereignisanzeige	Zusätzliche Ereignisquellen	●

Table 2.6: Modifikationen der NT-Standardwerkzeugen für ihre Verwendung in einer WTS-Umgebung

Seite 126

Sicherheitsmaßnahme	Niedrig	Mittel	Hoch
WTS-Installation auf einer NTFS-Partition	●	●	●
Regelmäßiges Sicherung des WTS-Systems	●	●	●
Deaktivieren unnötig freigegebener Verzeichnisse	●	●	●
Systemrichtlinien für die Benutzerkonten setzen	●	●	●
Überwachung immer kurzzeitig nach Installationen und Konfigurationsänderungen einschalten	●	●	●
Schutz des Windows Terminal Servers durch eine Firewall	○	●	●
Deaktivieren der Boot-Option über Diskette	○	●	●
Deaktivieren des BIOS-Setup-Prompt	○	●	●
Einbetten des Windows Terminal Servers in eine Domäneninfrastruktur mit entsprechenden Vertrauensstellungen	○	●	●
Deaktivieren nicht benötigter Netzwerkanbindungen	○	●	●
Überwachung der Standardereignisse	○	●	●
Als Administrator den Besitz aller Verzeichnisse und Dateien übernehmen und dokumentieren	○	●	●
Standardprofil oder verpflichtende Profile für Benutzerkonten einrichten	○	●	●
Das Anmelden für unbenutzte Gruppen verbieten	○	●	●
Anlegen einer Notfalldiskette. Falls Rdisk aufgrund der Registrierungsgröße nicht verwendet werden kann, müssen andere Werkzeuge genutzt werden (z.B. aus dem Resource Kit).	○	●	●
Spezielles Absichern der Daten für Internet-Dienste	○	●	●
Entfernen des FTP-Dienstes vom System	○	●	●
Internet-Dienste im Kontext eines Benutzers ablaufen lassen	○	●	●
Entfernung nicht benötigter Netzwerkprotokolle und -dienste	○	○	●
Veränderung der Standardeinstellungen für die Systemüberwachung	○	○	●
Aufnahme von wichtigen Dateien und Verzeichnissen in die Systemüberwachung	○	○	●
Anzeigen einer Sicherheitsmeldung bei jedem Anmelden	○	○	●
Vorgeben eines initiales Programm oder Skript beim Start einer Benutzersitzung	○	○	●
Löschen von nicht benötigten Netzwerk-Clients	○	○	●

Table 4.4: Mögliche Sicherheitsmaßnahmen für einen WTS

Seite 144

Clients	RDP	ICA
PCs unter Windows NT	●	●
PCs unter Windows 95/98	●	●
PCs unter Windows 3.11	●	●
PCs unter DOS und Windows 3.1	○	●
PCs unter OS/2	○	●
Macintosh	○	●
Computer unter UNIX (Sun, HP, DEC, IBM, SGI, SCO, Linux)	○	●
WWW-Browser (Internet Explorer, Netscape)	○	●
Windows-based Terminals unter Windows CE	●	●
Sonstige Terminals unter Windows CE, DOS, UNIX usw.	○	●
Netzwerk-Terminals	○	●
Set-Top-Boxen und drahtlose Geräte	○	●

Table 5.1: Die verfügbaren Clients für RDP und ICA

Transportprotokolle und Verbindungsarten	RDP	ICA
TCP/IP	●	●
IPX/SPX	○	●
NetBEUI	○	●
Verbindung im LAN	●	●
Verbindung im WAN	●	●
Verbindung über die serielle Schnittstelle (asynchron)	○	●
Direkte Modemverbindung	○	●
Modemverbindung über RAS	●	●
Suchliste der verfügbaren Multiuser-Server	○	●

Table 5.2: Transportprotokolle und Verbindungsarten für RDP und ICA

Seite 145

Verfügbare Systemeigenschaften	RDP	ICA
Systemklänge (Beep)	●	●
16-bit Stereoklang (WAV, MIDI, AVI)	○	●
Unterstützung für das Abspielen von Videos	○	●
Kontrolle der Multimedia-Bandbreite	○	●
Umlenken der COM-Anschlusszuordnung (seriell)	○	●
Umlenken der Druckeranschlusszuordnung (parallel)	(●)	●
Nahtlose Neuordnung von Laufwerksbuchstaben	○	●
Umlenken der Laufwerkszuordnung	○	●
Umlenken der Zwischenablage	(●)	●
Zwischenspeichern von Bitmaps (Bitmap-Caching)	○	● ▶



Verfügbare Systemeigenschaften	RDP	ICA
Randlose Anwendungsfenster	○	●
Automatische Wiederverbindung von Benutzersitzungen	(●)	●
Netzwerkumgebung für Programme (Program Neighborhood)	○	●

Table 5.3: Die verfügbaren Systemeigenschaften für RDP und ICA. Die Klammern deuten geplante Eigenschaften für folgende Versionen von RDP an (Stand: Windows 2000 Server Beta 3)

Verwaltung und WWW-Unterstützung	RDP	ICA
Spiegeln von Benutzersitzungen	(●)	●
Taskleiste für das Spiegeln von Benutzersitzungen	○	●
Vorkonfigurierbare Client-Einstellungen	○	●
Automatisches Aktualisieren der Client-Software	○	●
Dienst für das Ressourcen-Management	○	○ / ●
Dienst für das Installations-Management	○	○ / ●
Lastverteilung auf mehrere Server	○	○ / ●
Veröffentlichen von Anwendungen in das WWW	○	●
Anwendungszugriff aus WWW-Browsern (IE und Netscape)	○	●

Table 5.4: Verwaltung und WWW-Unterstützung für RDP und ICA. Die Klammer deutet eine geplante Eigenschaft für folgende Versionen von RDP an (Stand: Windows 2000 Server Beta 3). Die mit beiden Symbolen gekennzeichneten ICA-Eigenschaften benötigen eine Zusatzlizenz

Seite 155 / 156

Option	Verbindungsspezifische Einstellungen	Benutzerspezifische Einstellungen	Clientspezifische Einstellungen
Werkzeuge	Citrix-Verbindungs-konfiguration	Benutzer-Manager für Domänen	ICA-Verbindungen
TCP/IP-Protokoll	●	○	○
Asynchrones Protokoll (Modem)	●	○	●
IPX/SPX-Protokoll	●	○	●
NetBEUI-Protokoll	●	○	●
Konfiguration der verwendeten LAN-Adapter	●	○	○
Zähler für maximale Verbindungen	●	○	○
Protokollierung	●	○	○
Zeitlimits für Verbindungen	●	●	○
Zeitlimits für getrennte Verbindungen	●	●	○
Zeitlimit für Leerlauf	●	●	○
Sicherheit (Verschlüsselung)	●	○	○
Anmeldung verbieten	●	●	○
Automatisches Anmelden	●	○	○
Initiales Programm	●	●	●
Überschreiben von Benutzerprofilen	●	○	●

Option	Verbindungsspezifische Einstellungen	Benutzerspezifische Einstellungen	Clientspezifische Einstellungen
Werkzeuge	Citrix-Verbindungs-konfiguration	Benutzer-Manager für Domänen	ICA-Verbindungen
Behandlung unterbrochener Verbindungen	●	●	●
Automatische Wiederaufnahme von Verbindungen	●	●	○
Spiegeln von Benutzersitzungen auf andere Clients (Shadowing)	●	●	●
Beschränkung der Audiobandbreite	●	○	●
Zuordnung von Client-Geräten	●	●	○

Table 5.7: ICA-Konfiguration mit verschiedenen Werkzeugen

Seite 161

Registerkarte	Alle Server	Domäne	Server	Sitzung	Anwendung	Veröffentl. Anwendungen
Server	●	●	○	○	●	○
Benutzer	●	●	●	○	●	●
Sitzungen	●	●	●	○	○	○
Prozesse	●	●	●	●	○	○
Lizenzen	●	●	●	○	○	○
ICA-Gateways	●	○	○	○	○	○
ICA-Browser	○	○	●	○	○	○
Informationen	○	○	●	●	●	○
Cache	○	○	○	●	○	○
Anwendungen	○	○	○	○	○	●

Table 5.8: Angezeigte Registerkarten mit Informationen in der Citrix Server-Administration in Abhängigkeit des gewählten Objekts aus der Strukturliste

Seite 179

Der 32-bit-Client »Program Neighborhood«

Als Beispiel soll nun der 32-bit-Client für Windows etwas genauer betrachtet werden. Hier ist die »Netzwerkumgebung für Programme« (Program Neighborhood) für die Konfiguration der Verbindung sehr wichtig (Abbildung 5.34). Nach der Standardinstallation der Client-Software über einen Assistenten erlaubt dieses Werkzeug die Einrichtung von Verbindungsoptionen. Danach genügt ein Doppelklick mit der Maus, um eine Verbindung aufzunehmen und eine Benutzersitzung zu starten. Die Optionen der Program Neighborhood betreffen hierbei sowohl die direkte Anbindung von WTS-Desktops als auch die Verwendung von veröffentlichten Desktops und Anwendungen.