

Windows 2000 Terminal-Server

Einführung

Im Laufe der Zeit haben sich zwei Arten von Rechnernetzwerken entwickelt. Zum Einen das Peer-to-Peer- und zum Anderen das Client/Server Netzwerk. Beide Rechnernetzwerke basieren auf relativ leistungsfähigen Clientrechnern als Arbeitsstationen. Durch den Einsatz von Terminaldiensten wird die Nutzung von Clients mit geringen Ansprüchen an die Hardware und Software ermöglicht.

Die Terminaldienste auf einem Windows 2000-Server sorgen dafür, dass die Ausführung aller Clientanwendungen, die Datenverarbeitung und die Datenspeicherung auf dem Server erfolgt. Die Terminaldienste sind vollständig in Windows 2000 integriert und lassen sich auf zwei verschiedene Arten aktivieren:

- Remoteverwaltung

Der Systemadministrator hat über die Remoteverwaltung administrativen Zugriff auf jeden Windows 2000-Server über eine beliebige TCP/IP Verbindung. Er kann Datei- und Druckerfreigaben verwalten, auf einen anderen Computer die Registrierung bearbeiten und alle sonstigen Aufgaben erledigen, die er normalerweise direkt am Server über die Konsole durchführt.

Der Remoteverwaltungsmodus installiert lediglich die Remotezugriffskomponenten der Terminaldienste, aber keine Anwendungsfreigabekomponenten.

- Anwendungsserver

Beim Einsatz eines Terminal-Servers als Anwendungsserver wird das Konzept verfolgt, dass auf einem zentralen Server viele Benutzer gleichzeitig angemeldet sind und interaktiv mit den dort installierten Anwendungen arbeiten. Alle Anwendungen laufen ausschließlich auf dem Server ab. Den Zugriff auf einen Terminal-Server erhält der Benutzer über ein Netzwerk und über sogenannte "Schlanke Clients", die nur über Grundfunktionen verfügen und möglichst einfach zu verwalten sind. Diese "Schlanken Clients" werden auch Terminals genannt. Die Terminals dienen nur der grafischen Darstellung der Anwendungen, sowie die Benutzerinteraktion über Tastatur und Maus. Bei Bedarf können noch zusätzliche Ein- und Ausgabegeräte eingebunden werden.

Im Gegensatz zur Vorgängerversion (Windows NT 4.0 - Terminal Server Edition) muß für die Mehrbenutzeroption kein eigenes Betriebssystem erworben werden, sondern nur eine integrierte Komponente aktiviert werden. Es existiert für einen oder mehrere Benutzer nur noch ein gemeinsamer Systemkern.

Eine Mehrbenutzerumgebung stellt sich wie folgt dar:

1. Windows 2000 Terminal-Server:

Ein Windows 2000 Server mit installierten Terminaldiensten.

2. Kommunikationsprotokoll:

Das Standardprotokoll RDP (Remote Desktop Protocol) ermöglicht es den Clients, auf den Windows 2000 Terminal-Server zuzugreifen. Es basiert auf der Protokollfamilie T-120. RDP ist ein mehrkanalfähiges Protokoll, das

separate virtuelle Kanäle für die Übertragung der Kommunikation serieller Geräte und von Daten vom Server sowie verschlüsselter Daten von Tastatur und Maus des Clients erlaubt.

3. Thin Clients:

Ein Client-Gerät oder eine Client-Software. Ermöglicht den Zugriff auf einen Windows 2000 Terminal-Server über das Netzwerk und Darstellung des Desktop und die Eingabe über Tastatur und Maus.

Verwaltungsprogramme

Bei der Installation der Terminaldienste für Windows 2000 werden zusätzliche Verwaltungsprogramme zum Ordner Verwaltung hinzugefügt. Die folgenden Programme werden installiert:

- Terminaldienste-Clientinstallation

Mit diesem Programm werden Installationsdisketten für die Terminaldienst-Clientsoftware auf folgenden Plattformen erstellt. Windows für Workgroups, Windows 95, Windows 98, und Windows NT.

- Terminaldiensteverwaltung

Mit diesem Programm können alle Windows 2000-Server verwaltet werden, auf denen die Terminaldienste ausgeführt werden. Administratoren können die aktuellen Benutzer, Server und Prozesse anzeigen, Nachrichten an bestimmte Benutzer senden, die Remotesteuerung ausführen und Prozesse beenden.

- Terminaldienstekonfiguration

Mit diesem Programm wird die RDP-Konfiguration (Remote Desktop Protocol) verwaltet. Die verfügbaren Optionen umfassen Einstellungen zur Verschlüsselung von Verbindungen, Anmeldeeinstellungen, Zeitlimits, Programme, die nach erfolgreicher Anmeldung gestartet werden, Remotesteuerungsoptionen, Windows-Druckerzuordnung, LPT-Anschlußzuordnung.

- Terminaldienstelizenzen

Mit diesem Programm werden die Clientzugriffslizenzen für Windows 2000 Terminaldienste gespeichert und überwacht.

Anmeldung an einem Terminal-Server

Die Anmeldung auf dem Client eines Terminal-Servers unterscheidet sich grundsätzlich nicht von dem entsprechenden Vorgang unter der Standardversion von Windows 2000 durch Eingabe des Benutzernamens und des Kennwortes. Benutzer, die nur eine einzige Anwendung, z.B. eine Datenbank, benötigen, können direkt nach dem Start auf die geöffnete Anwendung zugreifen. Dazu muß der Terminal-Server entsprechend konfiguriert werden. Mit dem Client-Verbindungsmanager wird auf Benutzerebene festgelegt, welche Anwendung automatisch startet.

Es können auch Verbindungen ohne Eingabe von Benutzername und Kennwort zugelassen werden. Diese Verbindungsmethode sollte jedoch nur für Benutzer vorgesehen werden, die auf direktem Weg in eine Anwendung (z.B. Word, Access, Excel) gelangen sollen. Voraussetzung sollte aber ein zusätzliches Zugangskennwort für die auf dem Terminal-Server

bereitgestellte Anwendung sein. Diese Form der Anmeldung sollte jedoch mit größter Sorgfalt eingesetzt werden. Über ein unbeaufsichtigtes Client-System kann jeder, ohne Kenntnis von Kennworten, in eine Domäne eindringen. Dies stellt eine Gefährdung der Systemsicherheit dar.

Desweiteren sollten noch folgende Faktoren bei der Einrichtung von Terminaldiensten berücksichtigt werden:

- Kein Einsatz von Smartcards

Bei der interaktiven Anmeldung unter Windows 2000 kann der Benutzer im Active Directory-Netzwerk anhand eines auf einer Smartcard gespeicherten X.509-Zertifikats (Version 3) in Kombination mit einem privaten Schlüssel authentifiziert werden. Für einen Benutzer, der sich über den Terminaldienst authentifiziert ist diese Funktion nicht verfügbar. Diese Ausnahmeregelung kommt auch für andere hardwarebasierte Authentifizierungsverfahren zum Tragen.

- Informations- und Terminaldienste

Bei den Informations- und Terminaldiensten sollten anonyme Zugriffe (Anonymous) über das FTP-Protokoll (File Transfer Protocol) deaktiviert werden, damit ungesicherte Zugriffe auf das Dateisystem unterbunden werden. Läuft anonymes FTP auf demselben Rechner wie die Terminaldienste, kann ein Eindringling eine Datei im Anonymous-FTP-Bereich plazieren und den Terminal-Server dazubringen, sie auszuführen.

Dateisystem

Aus Gründen der Sicherheit sollte NTFS als einziges Dateisystem auf dem Terminal-Server eingesetzt werden. Auf FAT-Partitionen sollte ganz verzichtet werden. Das FAT-System bietet keinerlei Sicherheiten auf Benutzer- und Verzeichnisebene. Bei mit NTFS formatierten Partitionen können Zugriffe auf Unterverzeichnisse auf bestimmte Benutzer oder Benutzergruppen begrenzt werden. Bei einem Mehrbenutzersystem wie den Terminaldiensten ist dieser Aspekt von entscheidender Bedeutung. Ohne die Sicherheitsmechanismen von NTFS können alle Benutzer auf sämtliche Verzeichnisse und Dateien auf dem Terminal-Server zugreifen.

Gruppenrichtlinien und Terminaldienste

Benutzer- und Computereinstellungen wurden in Windows NT 4.0 mit dem Systemrichtlinien-Editor konfiguriert und in der Registrierdatenbank von Windows NT gespeichert. Das Konzept der Systemrichtlinien wird in Windows 2000 durch die Gruppenrichtlinien ersetzt und sind Bestandteil der Active Directory Services. Active Directory ist der Verzeichnisdienst für Windows 2000 Server und speichert Informationen über Netzwerkobjekte, wie z.B. Benutzer, Computer und freigegebene Ressourcen.

Gruppenrichtlinien dienen dazu, die System- und Anwendungseinstellungen für Gruppen von Benutzern und Rechnern von einer zentralen Stelle aus zu definieren. Zu diesen Einstellungen gehören Softwarerichtlinien, Skripts (Hoch- und Herunterfahren des Computers - An- und Abmelden des Benutzers), Benutzerdokumente und -einstellungen, sowie Sicherheitseinstellungen. Gruppenrichtlinien werden mit Hilfe des Werkzeugs für die Verwaltung von Active Directory-Benutzern und - Computern als Eigenschaft einer Domäne oder Organisationseinheit (OU) definiert. Die von der Gruppenrichtlinie festgelegten Informationen sind in

einem Gruppenrichtlinienobjekt (Group Policy Object - GPO) enthalten. Das GPO wird mit einem oder mehreren Active Directory-Objekten, z.B. einer Site, Domäne oder OU verbunden, so dass eine zentrale Verwaltung von Richtlinienoptionen möglich ist.

Beim Einsatz von Terminaldiensten und gleichzeitigem Nutzen von Windows 2000 Professional sind die Gruppenrichtlinien besonders zu beachten, da sowohl der Windows 2000- als auch der Terminal-Server dieselben Richtlinien nutzt. Auf einem Server, auf dem die Terminaldienste ausgeführt werden, sollten separate Richtlinien angewandt werden. Daher ist es notwendig, alle Rechner, auf denen Terminaldienste ausgeführt werden, in eine separate Organisationseinheit (OU) zu legen. Mit Hilfe der Gruppenrichtlinien kann der Zugriff auf die Terminaldienstanwendungen auf zwei Arten gesteuert werden:

1. Verbindliche Profile

Verbindliche Profile legen fest, welche Anwendungen der Benutzer sehen und starten kann.

2. Gruppenrichtlinien

Mit Hilfe der Gruppenrichtlinien können Benutzer daran gehindert werden, Anwendungen über den Windows Explorer oder mit dem Befehl "Ausführen" zu öffnen. Da die Richtlinien auf Domänenbasis gelten, kann sowohl der Rechner des Benutzers als auch seine Terminalsitzung beeinflusst werden. Zuerst wird die Benutzerrichtlinie für die Domäne angewandt und dann mit der Rechnerrichtlinie verbunden. Erstellt ein Administrator eine Richtlinie auf der Basis einer Benutzer-ID oder einer Sicherheitsgruppe und implementiert diese, gilt sie für diesen Benutzer bzw. die Gruppe unabhängig davon, ob diese(r) einen Rechner oder einen Terminaldienstclient benutzt.

Um eine größere Systemsicherheit zu erreichen, können die beim Terminaldienst mitgelieferten Benutzerrechte geändert werden. Damit sich ein Benutzer bei einem Terminal-Server anmelden kann, muss er lokale Anmelderechte für den Server besitzen. Werden die Terminaldienste im Remoteverwaltungsmodus konfiguriert, erhalten nur die Administratoren Rechte auf dem Rechner. Ist der Server als Anwendungsserver konfiguriert, werden allen Mitgliedern der Gruppe "Benutzer" Rechte gewährt. Da Windows 2000 alle Domänenbenutzer in die Gruppe "Benutzer" einschließt, können sich alle Benutzer bei den Terminaldiensten im Anwendungsservermodus anmelden. Mit Hilfe der Terminaldienstkonfiguration können die Anmeldeberechtigungen für Benutzer und Gruppen geändert werden.

Benutzer, die Zugriff auf die Terminaldienste bekommen, das RDP-Protokoll einsetzen und sich interaktiv bei einem terminaldienstfähigen Server anmelden, werden automatisch in die lokale Benutzergruppe der Terminaldienste aufgenommen. Diese lokale Gruppe wird bei der Erstkonfiguration der Terminaldienste angelegt. Mitglied dieser Gruppe ist der Benutzer aber nur solange, wie er interaktiv beim Server angemeldet ist.

Der Anwendungsmodus der Terminaldienste sollte nicht für Domänencontroller aktiviert werden, da die Richtlinien für Benutzerrechte dann für alle Domänencontroller innerhalb der Domäne gelten. Wenn die Terminaldienste z.B. gemeinsam mit anderen Anwendungen benutzt werden sollen, müssen sich die Benutzer lokal anmelden können. Ist der Server auf dem die Terminaldienste laufen ein Domänencontroller, können

sich die Benutzer lokal bei allen Domänencontrollern in der Terminaldienstdomäne anmelden.

Administratoren

Die Mitglieder der Administratorengruppe eines Terminal-Servers legen fest, welche Benutzer auf welche Anwendungen mit welchen Rechten Zugriff erhalten. Der überwiegende Teil dieser Kontrollmechanismen gehört zu den Standardrechten eines Administrators für Windows 2000 Server. Diese Rechte werden beim Einsatz der Terminaldienste um die folgenden Komponenten erweitert:

- Serververwaltung

Über das Verwaltungsprogramm zur Terminaldienstkonfiguration können Benutzerberechtigungen und Sitzungsaktivitäten eingerichtet sowie Vorgänge und Sitzungen getrennt werden.

- Benutzersteuerung

Benutzerberechtigungen für Terminaldienste werden mit der Terminaldienstkonfiguration erteilt. Spezifische Profile für Terminaldienste können mit dem erweiterten Benutzer-Manager erstellt werden.

- Sitzungssteuerung

Die Terminaldienstverwaltung dient zur Überwachung der aktiven Benutzer, Sitzungen und Prozesse. Es können Sitzungen gespiegelt und die Trennung von Verbindungen erzwungen werden.

- Installation von Anwendungen

Bei Terminal-Server, die im Anwendungsfreigabemodus betrieben werden, sind nur Administratoren befugt, Anwendungen zu installieren.

Konfiguration von Terminaldienstbenutzern

Die Konfiguration von Terminaldienstbenutzern erfolgt wie die Konfiguration lokaler oder Active Directory-Benutzer unter Windows 2000. Bei der Installation der Terminaldienste auf einem Rechner erscheinen auf der Eigenschaftenseite des Benutzers zwei weitere Registerkarten mit den Eigenschaften: "Remoteüberwachung" und "Terminaldienstprofile".

Benutzerberechtigungen

Den Zugriff von Benutzern und Gruppen auf die Terminaldienste werden durch das Festlegen von Zugriffsberechtigungen gesteuert. Es wird unterschieden nach:

Vollzugriff

- Abfragen von Informationen über eine Sitzung
- Ändern von Verbindungsparametern
- Zurücksetzen (oder Beenden) einer Sitzung
- Remoteüberwachung der Sitzung eines anderen Benutzers
- Anmelden bei einer Sitzung auf dem Server
- Abmelden eines Benutzers von einer Sitzung
- Senden einer Nachricht an die Sitzung eines anderen Benutzers
- Verbinden mit einer anderen Sitzung
- Trennung einer Sitzung

Benutzerzugriff

- Anmelden bei einer Sitzung auf dem Server
- Abfragen von Informationen über eine Sitzung
- Senden von Nachrichten an Sitzungen anderer Benutzer
- Verbinden mit einer anderen Sitzung

Gastzugriff

- Der Gastzugriff erlaubt Benutzern lediglich das Anmelden bei einer Sitzung auf dem Server.

Unter einer Option des Startmenüs kann der Benutzer sicherheitsrelevante Einstellungen vornehmen, sofern er die hierzu benötigten Rechte besitzt. Diese spezielle Option ist nur auf dem Terminal-Client sichtbar und über "Start - Einstellungen - Windows Sicherheit" zu erreichen.

Folgende Einstellungen können vorgenommen werden:

- Änderung des Kennworts, wobei dieses sowohl zu einem lokalen als auch zu einem netzwerkbasierten Benutzerkonto gehören kann.
- Kennwortgeschütztes Sperren des Bildschirms und aller Eingabegeräte.
- Abmelden des aktuell angemeldeten Benutzers.
- Herunterfahren des Rechners, sofern der angemeldete Benutzer die hierzu benötigten Rechte besitzt.
- Betrachtung und Modifikation aller Prozesse des aktuell angemeldeten Benutzers.

Client-Server-Verbindung

Damit die Datenübertragungen zwischen Terminaldienstclients und -servern möglichst sicher sind, sollten diese verschlüsselt werden. Es stehen drei verschiedene Verschlüsselungsarten zur Verfügung:

- Niedriger Verschlüsselungsgrad

Bei diesem Verschlüsselungsgrad wird nur der Datenfluss vom Client zum Server unter Verwendung des RC4 Algorithmus und eines 56-Bit-Schlüssels verschlüsselt. Die Datenübertragung vom Server zum Client erfolgt unverschlüsselt.

- Mittlerer Verschlüsselungsgrad

Bei einem mittleren Verschlüsselungsgrad wird der Datenfluss in beide Richtungen mittels RC4-Algorithmus und einem 56-Bit-Schlüssel verschlüsselt.

- Hoher Verschlüsselungsgrad

Früher konnte der Datenfluss nur in der nordamerikanischen Version in beide Richtungen mit dem RC4-Algorithmus und einem 128-Bit-Schlüssel verschlüsselt werden. Ab Februar 2000 wurden die US-Exportbestimmungen für starke Verschlüsselung gelockert, wodurch die 128-Bit-Option auch auf dem internationalen Markt verfügbar wurde.

Terminaldienst und Internet

Das RDP (Remote Desktop Protocol) unterstützt TCP/IP Verbindungen zwischen Terminaldienstclient und -server. Es können somit Verbindungen über Netzwerk- und DFÜ-Verbindungen, im lokalen LAN oder über eine VPN (Virtual-Private-Network)-WAN-Verbindung hergestellt werden. Um das Mitlesen der übertragenen Daten zu verhindern, sollten diese

Verbindungen überwiegend verschlüsselt erfolgen. Hierzu bietet sich das L2TP-Protokoll (Layer-2 Tunneling Protocol) oder das PPTP-Protokoll (Point-to-Point Protocol) an. Beide Protokolle verwenden das ESP-Protokoll (IP Encapsulating Security Payload) von IPSec (Internet Protocol Security), das in Windows 2000 implementiert ist, zum Verschlüsseln und Authentifizieren, um so mit die Vertraulichkeit von Netzwerken zu gewährleisten.

Firewall

Nach heutigen Standards werden in Unternehmen Firewalls aus Sicherheitsgründen eingesetzt, um das Intranet gegen Angriffe von außen zu schützen. Die Zugänge nach außen und innen werden über sogenannte Ports gewährleistet. Die Firewall sollte dahingehend konfiguriert werden, die "offenen" Ports auf ein Mindestmaß zu reduzieren, um den größtmöglichen Schutz gegenüber Attacken aus dem Internet zu erreichen. Beim Einsatz von Terminaldiensten besteht aber nun generell die Notwendigkeit, dass der Port 3389 für die RDP-Verbindungen zwischen Client und Server offengehalten wird. Um zu verhindern, dass dieser Port internetweit genutzt wird, sollte sich der Nutzer des Terminaldienstes explizit gegenüber der Firewall authentisieren.

Einsatzmöglichkeiten eines Windows 2000 Terminal-Servers

Internetzugang über Terminal-Server

Der direkte Zugang zum Internet (insbes. WWW und ftp) vom Arbeitsplatz aus birgt eine Reihe von Risiken für die auf dem entsprechenden PC verarbeiteten oder von dort aus zugreifbaren Daten. Handelt es sich um (sensible) personenbezogene Daten, sind Maßnahmen zu treffen, um diese Gefahren auszuschließen oder ausreichend zu begrenzen.

Eine mögliche technische Lösung besteht darin, den Internetzugang vom PC am Arbeitsplatz auf einen speziell dafür eingerichteten Server zu verlegen. Auf diesem Server werden weder personenbezogene Daten verarbeitet noch sind diese ohne weitere Authentisierungsmaßnahmen zugreifbar. Die Gefahren, die durch den Internetzugang bestehen, wirken sich daher zunächst nur auf den Server (z.B. hinsichtlich seiner Verfügbarkeit) aus, nicht jedoch auf andere Rechner (Arbeitsplatz-Rechner oder andere Server). Diese Risiken sind insofern hinnehmbar. In diesem Fall kann der Server über einen freien Internet-Zugang verfügen, der nicht über einen Proxy hinsichtlich bestimmter URL gefiltert wird. Den Schutzmaßnahmen auf dem Server sollte jedoch eine besondere Beachtung geschenkt werden.

Dieser spezielle Server für den Internetzugang wird als Terminal-Server betrieben, so dass von den eigentlichen Arbeitsplatz-PC aus auf den Server nahezu so zugegriffen werden kann, als würde man lokal an dem Server arbeiten. Daher kann der dort bestehende Internetzugang vom Arbeitsplatz aus genutzt werden, ohne dass eine direkte Verbindung vom Arbeitsplatz ins Internet besteht:

Weder ist es auf diesem Weg möglich, den Arbeitsplatz-PC vom Internet aus direkt zu kontaktieren noch können Daten aus dem Internet auf den PC oder vom PC ins Internet transferiert werden. Der Zustand des Arbeitsplatz-PC wird durch diese Form des Internet-Zugangs also nicht dauerhaft geändert.

Allerdings bedeutet dies, dass auch gewünschte Datentransfers nicht unmittelbar möglich sind. Der Download eines Dokuments aus dem Internet zur Weiterverarbeitung auf dem PC muss daher in zwei Schritten erfolgen: zunächst der Download auf den Terminal-Server, anschließend

der Transfer per Datenträger auf den PC. Entsprechendes gilt für Uploads. Terminal-Server sind in der Lage, mehrere Sitzungen gleichzeitig zu bedienen, so dass sich mehrere Benutzer einen Server teilen können. Wieviele Benutzer ein bestimmter Server verkraften kann, hängt von verschiedenen Hard- und Softwarefaktoren ab.

Telearbeit

Bei der Telearbeit ist der gesicherte Zugriff auf Rechner innerhalb eines Netzwerkes (z.B. Firmennetzwerk, Verwaltungsnetzwerk) von außen zu gewährleisten. Der "klassische Arbeitsplatz" ist durch den Einsatz modernster Technik einem stetigen Wandel unterzogen. In immer mehr Projekten und Arbeitsaufgaben wird es erforderlich, Zugriff vom häuslichen Arbeitsplatz auf die Daten und die Infrastruktur eines bestehenden Netzwerkes zu erhalten. Durch den Einsatz von Terminaldiensten kann der Zugriff auf die benötigten Daten in einem bestehenden Netzwerk über einen Terminal-Server gewährleistet werden.

Realisiert werden kann dies beispielsweise über den Zugriff einer ISDN-Leitung, wobei der Datenverkehr verschlüsselt werden sollte und der Benutzer sich am Firmen- bzw. Verwaltungsnetz explizit authentisieren muß.