Kapitel 1

Einführung in Terminaldienste von Windows Server 2008

In diesem Kapitel:

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

Es gibt verschiedene Gründe, dieses Buch zu lesen. Vielleicht sind Sie bereits mit Terminalserver vertraut und möchten wissen, was Terminaldienste in Windows Server 2008 für Sie tun können. Eventuell arbeiten Sie bereits mit Windows Server 2008 und sind daran interessiert, was all diese Webzugriffe, Gateways und Terminalserver tun. Oder Sie haben seit Längerem von Terminaldiensten gehört und möchten davon profitieren, indem Sie Terminaldienste in Ihre Umgebung einbinden. Es stellt sich nun die Frage: Was können Terminaldienste für Sie tun, was sich mit verwalteten Desktops nicht realisieren lässt?

Welcher Grund auch zutreffen mag – dieses Buch wird das richtige für Sie sein.

Dieses Kapitel bereitet die Bühne für den übrigen Teil des Buchs. Um die Evolution von Terminaldiensten zu verstehen, müssen Sie wissen, woher sie kommen und wie die Umgebung aussieht, in der sie operieren. Wenn Sie verstehen möchten, was Sie mit Rollen und Rollendiensten anfangen können, müssen Sie die wesentlichen Ziele der Terminaldienste in Windows Server 2008 und die Szenarios, für die sie konzipiert sind, kennen. Und da Terminaldienste keine eigenständige Komponente verkörpern, sondern zu einer breit angelegten Windows-Infrastruktur gehören, erfahren Sie, wie Rollendienste für Terminaldienste mit anderen Rollen interagieren.

Am Ende dieses Kapitels wissen Sie,

- was Windows Server 2008 für die Unterstützung einer Umgebung für Terminaldienste einbindet
- welche Szenarios die Rollendienste für Terminaldienste konzeptionell unterstützen sollen
- wie Rollendienste für Terminaldienste miteinander interagieren
- wie Rollendienste für Terminaldienste mit anderen Windows Server-Rollen zusammenarbeiten können
- welche Schnittstellen für unabhängige Softwareanbieter (Independent Software Vendors, ISVs) und Kunden zur Verfügung stehen, die zugeschnittene Projekte auf der Basis von Terminaldiensten erstellen möchten, und welche Möglichkeiten diese Schnittstellen bieten.

Woher kommt Terminalserver?

Wenn Sie Terminaldienste erstmals mit Windows Server 2008 sehen, werden Sie kaum noch Spuren der frühen Realisierungen erkennen. Wie bei Windows Server selbst hat sich auch bei Terminaldiensten im Lauf der Jahre eine ganze Menge geändert. Es ist nicht nötig, die umfangreiche Featureliste für jede Edition durchzugehen. Zweckmäßig ist es aber zu sehen, wie sich Mehrbenutzer-Windows seit den ersten Anfängen Mitte der 1990er Jahre entwickelt hat.

Die ursprüngliche MultiWin-Architektur wurde vom Softwareunternehmen Citrix konzipiert, das Lizenzen für den Windows NT 3.51-Quellcode von Microsoft erworben hat, um Windows für Mehrbenutzer zu realisieren. (MultiWin geht auf das Betriebssystem OS/2 von IBM zurück, als Microsoft noch im OS/2-Projekt engagiert war. Windows hat sich durchgesetzt.) Citrix hat ein eigenes Produkt unter dem Namen WinFrame herausgebracht, das eine Mehrbenutzerversion von Windows NT 3.51 darstellte und vollkommen getrennt von dem Betriebssystem war, das Microsoft produziert hat.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

Erste Erfahrungen mit Mehrbenutzer-Windows

Christa hat 1997 erstmals mit Mehrbenutzer-Windows über WinFrame 1.7 in einem IBM-Schulungscenter im Hudson River Valley von New York Bekanntschaft geschlossen. Ursprünglich hatte das Schulungscenter in jedem Gästezimmer einen PC bereitgestellt (die Schulungen erstreckten sich über mehrere Tage, sodass es Hotelzimmer im Schulungscenter gab), und die Mitarbeiter hatten mit den Geburtswehen dieses Setups zu kämpfen. Sie sind dazu übergegangen, in allen Gästezimmern Thin Clients einzurichten (die mit den WinFrame-Servern verbunden waren), sodass die Gäste von ihren Zimmern aus arbeiten und E-Mails abrufen konnten. Beim Einchecken der Teilnehmer wurde für die jeweilige Person automatisch mit einem Skript ein Benutzerkonto erstellt. Aus heutiger Sicht ist es verständlich, dass dies ein recht voreiliges Unterfangen war und eine große Änderung gegenüber dem desktoporientierten Modell von Windows bedeutete.

Der Haken bei WinFrame liegt natürlich darin, dass es auf Windows NT 3.51 aufbaut. Microsoft kaufte 1995 die Lizenz von Citrix zurück und baute diesen Mehrbenutzerkern in das Basisbetriebssystem ein, um ein neues Produkt zu kreieren: Windows Server mit Mehrbenutzerfähigkeiten. Das Ergebnis war Windows NT Terminal Server Edition. Citrix stellte kein eigenständiges Produkt mehr bereit, veröffentlichte aber MetaFrame, das auf Terminal Server Edition in fast der gleichen Form aufsetzte wie heutzutage Citrix Presentation Server auf Windows Server läuft.

Terminal Server Edition war bestenfalls ein Ausgangspunkt. Das Betriebssystem war ziemlich einfach gestrickt, um es milde auszudrücken. Fast jede Installation von Terminal Server Edition lief mit aufgesetztem MetaFrame, da das Basisprodukt kaum mehr als ein Mehrbenutzer-Betriebssystem bereitstellte. Es fehlte selbst an grundlegender Funktionalität wie zum Beispiel der Zwischenablagezuordnung. Dass Terminal Server Edition und das Kernbetriebssystem unterschiedliche Produkte verkörperten, war weder für Microsoft noch für seine Kunden ein Vergnügen. Microsoft hatte es mit zwei Sätzen von Betriebssystem-Servicepacks zu tun, während Kunden ein separates Produkt kaufen mussten, um serverbasierte EDV zu testen, und mit zwei unterschiedlichen Servicepacks zu jonglieren, die nicht zur selben Zeit veröffentlicht wurden. (Der Vorteil dabei: Wenn es ein Problem mit Service Pack 6 für Windows NT 4.0 gab, war das Problem gelöst, indem das SP 6 für Terminal Server Edition veröffentlicht wurde.)

Der erste wirkliche Durchbruch bei Microsoft Terminaldiensten ist mit Windows 2000 Server zu verzeichnen. Zum ersten Mal waren Terminaldienste eine Serverrolle im grundlegenden Serverbetriebssystem und kein separates Produkt. Weshalb ist das so wichtig? Dafür gibt es mehrere Gründe. Erstens gehörte das Jonglieren mit inkompatiblen Servicepacks für Einzelbenutzer- und Mehrbenutzer-Betriebssysteme der Vergangenheit an. Zweitens gab es eine grundlegende Änderung in der Art und Weise, wie serverbasierte Verarbeitung und Remotezugriff wahrzunehmen waren. Wenn Sie vor Windows 2000 einen Windows-Server von der grafischen Benutzeroberfläche aus verwalten wollten, musste dies im Allgemeinen direkt von diesem Rechner aus erfolgen – es gab keine Möglichkeit für eine Remoteverwaltung mit dem Microsoft Remote Desktop Protocol (RDP). Das Problem dabei: Die Anzahl der Server, vor denen Sie im Laufe des Tages sitzen können, ist naturgemäß begrenzt, vor allem dann, wenn diese Server in verschiedenen Gebäuden – oder sogar in verschiedenen Städten – stehen. Windows 2000 Server führte die Remoteverwaltung als optionale Komponente ein, sodass Serveradministratoren die Server – selbst die in anderen Gebäuden – verwalten konnten, auch wenn sie nicht davor saßen. Das hat nicht nur die Arbeit für Serveradministratoren erleichtert, sondern kam auch den Terminaldiensten zugute, da es ein gutes Szenario für Remoteverwendung und Mehrbenutzerverarbeitung lieferte.

Hat man Terminaldienste im Anwendungsservermodus im Kernbetriebssystem verfügbar, heißt das auch, dass der Aufwand vergleichsweise gering ist, Terminalserver für Endbenutzer auszuprobieren – um einen Basispiloten einzurichten, genügt es, die Rolle im Anwendungsservermodus zu installieren und die Benutzer mit Notepad arbeiten zu lassen. Und da RDP in Windows 2000 Server zusätzliche Funktionalität wie zum Beispiel eine Clientdruckerumleitung und eine gemeinsame Zwischenablage für lokale und remote Sitzungen einführte, reichten allein die Tools im Kernbetriebssystem aus, um Terminalserver auszuprobieren und ein Gefühl dafür zu bekommen, wie Endbenutzer von der gemeinsamen Verarbeitung profitieren konnten.

Den nächsten großen Schritt markiert Windows Server 2003. Hier wurden einige Entscheidungen zum nächsten logischen Abschluss umgesetzt, die im Zeitrahmen von Windows 2000 Server getroffen wurden. Wenn Remoteverwaltung eine feine Sache ist, weshalb sollte sie dann nur eine optionale Komponente sein? Stattdessen wird sie für sämtliche Windows-Serverrollen aktiviert und für den Client als Option gelassen. Denn die Basisfunktionalität ist zwar in Windows 2000-Terminalserver nützlich, bietet aber keine ausgefeilte Clientunterstützung. Mit aktivierter Laufwerkzuordnung, vollem Farbumfang, Sound und anderen Features, die vorher nur mit Produkten von Drittanbietern verfügbar waren, kommt die Benutzeroberfläche auf Remotecomputern schon eher an die Desktopbenutzeroberfläche heran.

Eine weitere entscheidende Änderung in Windows Server 2003 betrifft den Bereich der Verwaltung. Windows 2000-Terminalserver ließen sich nur einzeln verwalten. Es war zwar möglich, sie remote zu konfigurieren, allerdings nicht gemeinsam. Windows Server 2003 hat einige Gruppenrichtlinieneinstellungen für das Konfigurieren und Verwalten von Terminalservern eingeführt, und die Terminalserververwaltung unterstützte die Verwaltung von Remoteservern.

Dieses Buch konzentriert sich zwar auf die Benutzeroberfläche, die den Servercomputern gemeinsam ist, und nicht auf den Client, doch sollten Sie wissen, dass in dieser Zeit auch die Terminaldienste auf der Clientseite Änderungen erfahren haben. Windows 2000 Professional hat keine eingehenden Remotezugriffsverbindungen unterstützt (von Windows 9*x* ganz zu schweigen), während dies in Windows XP und Windows Vista möglich ist. Durch die Unterstützung eingehender Remoteverbindungen ist es unter anderem möglich, Windows-Clients wie folgt zu verwenden:

- Remotezugriff von zuhause oder einem anderen Bereich des Gebäudes aus
- Remoteunterstützung
- Hosting von virtuellen Desktops

Remotezugriff von einem anderen Computer aus spiegelt die Realität wider, dass viele Benutzer mit mehr als einem Computer arbeiten – ja selbst im Heimbereich mehrere Computer vorhanden sind. Remoteunterstützung greift auf das Feature *Remoteüberwachung* der Terminaldienste – die Möglichkeit, einem zweiten Benutzer zu erlauben, eine Remotesitzung zu sehen oder sogar zu übernehmen – zurück, um Helpdesksupport selbst auf Desktops zu ermöglichen. Und schließlich ist das Hosting von virtuellen Desktops eine echte Konkurrenz zu Terminaldiensten, um eine gehostete Anwendungsumgebung bereitzustellen, wenn ein freigegebener Computer keine praktikable Option ist.

Terminaldienste erscheinen auch in den Clientversionen von Windows, selbst wenn Sie dies nicht erwarten. Es ist die Technologie, die schnelle Benutzerumschaltung und Remoteunterstützung (um nur zwei zu nennen) möglich macht.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

Kurz gesagt ist die Geschichte von Terminaldiensten die Geschichte dessen, wie Mehrbenutzerverarbeitung aus einer Technologienische herausgetreten ist und sich mehr zu einer Strategie entwickelt hat, die verschiedene Szenarios ermöglicht, die die Trennlinie zwischen PC und Datencenter verschwimmen lassen. Auch wenn sie nicht Terminaldienste heißen, sind Mehrbenutzercomputer und das Remotedesktopprotokoll zu entscheidenden Bestandteilen der Windows-Kernplattform geworden.

Was können Sie mit Terminaldiensten tun?

Der vorherige Abschnitt hat einen (recht kurzen) Überblick gegeben, woher serverbasiertes Windows kommt und wie es Bestandteil der Windows-Kernplattform sowohl für Client als auch Server geworden ist. Doch was tun Sie damit?

Prinzipiell trennen Terminaldienste die festen Verknüpfungen zwischen Ort und Funktion. Mit einem PC sind Sie absolut daran gebunden, was dieser Computer tun kann. Serverbasierte Technik eröffnet Ihnen flexiblere Möglichkeiten. Dies wirkt sich vorteilhaft auf Sicherheit, Standort und Geräteunabhängigkeit aus.

Die Sicherheit für Remotebenutzer verbessern

Vollkommen auf PCs ausgerichtete Rechentechnik hatte Probleme mit der Datensicherheit. Mehr und mehr Benutzer arbeiten auf Laptops und diese sind ja gerade für das Arbeiten unterwegs konzipiert. Allerdings sind Laptops mit den darauf gespeicherten Daten ein Sicherheitsrisiko, selbst wenn der Laptop durch Kennwörter gesichert ist. Sofern Sie den Laptop nicht ständig bei sich tragen – d.h. ihn beispielsweise auch zum Abendessen mitschleppen, anstatt ihn im Hotelzimmer zu lassen –, sind die Daten auf Ihrem Laptop diebstahlgefährdet. Und wenn jemand wirklich auf Ihren Laptop aus ist, spielt es auch keine Rolle, ob Sie ihn mit sich führen, ganz zu schweigen davon, dass Sie den Laptop versehentlich im Taxi oder im Zug liegenlassen. Es passiert eben.

Befinden sich die Daten auf dem Laptop und Sie verlieren ihn, sind die Daten weg. Die nahe liegende Lösung ist: Behalten Sie die Daten nicht auf dem Laptop – speichern Sie sie stattdessen im Datencenter. Doch wenn Sie auf das Datencenter von einem Remotestandort aus zugreifen und mit großen Dateien arbeiten (welche Datei ist bei der heutzutage üblichen umfangreichen Formatierung nicht groß?), ist man schon versucht, die Datei auf dem lokalen Laufwerk zu behalten, während man unterwegs damit arbeitet, und sie in das Netzwerk zurückzukopieren, wenn die Bearbeitung abgeschlossen ist. Endergebnis: Die Daten befinden sich auf dem lokalen Laufwerk und Sie stehen wieder am Anfang.

Informationsunsicherheit

Praktisch ist es kaum möglich, vertrauliche Informationen nur für die Personen innerhalb der vier Wände des Büros zugänglich zu machen, doch es zeigt sich immer wieder, was passiert, wenn diese Informationen das Datencenter verlassen. Im November 2007 hatte die britische Steuerbehörde zwei CDs mit persönlichen Daten – Bankverbindungen, Geburtsdaten, Adressen und Namen aller Kindergeldempfänger (25 Millionen Briten) – an den Rechnungshof geschickt, die aber auf dem Postweg verloren gingen und nicht wieder aufgetaucht sind. Und das war auch nicht das erste Mal, dass vertrauliche Daten auf einem verlegten Laptop oder anderen portablen Medien verschwunden sind. ▶

Nicht immer ist es machbar, sensible Informationen nur im Datencenter zu speichern, sodass sie außerhalb des Umkreisnetzwerks nur über eine sichere Verbindung zu einem Terminalserver zugänglich sind. Manchmal müssen die Informationen auch verfügbar sein, selbst wenn keine Netzwerkverbindung besteht. Ist es aber praktikabel, sollten die Informationen aus Sicherheitsgründen auch dort gespeichert werden, wo die Wahrscheinlichkeit am geringsten ist, dass sie gefährdet sind, gestohlen werden oder verloren gehen: im Datencenter.

Dieses Dilemma lässt sich beispielsweise dadurch lösen, dass *alles* im Datencenter untergebracht wird, einschließlich der Anwendungen, mit denen die vertraulichen Dokumente bearbeitet werden. Befinden sich sowohl die Anwendungen als auch die vertraulichen Daten im Netzwerk, ist es entweder unmöglich, die Daten lokal zu bearbeiten (weil keine geeignete Anwendung lokal installiert ist), oder kaum sinnvoll, weil es keinen Grund gibt, die Remotedatei auf den lokalen Computer herunterzuladen, um ein flüssigeres Arbeiten zu ermöglichen. Letztlich bleiben keine vertraulichen Daten auf dem Clientcomputer zurück und alles spielt sich innerhalb der Grenzen des Datencenters ab.

HINWEIS Bei genügend großer Entfernung oder genügend langsamer Internetverbindung ist die Remoteverbindung ebenfalls langsam. Und wenn die Netzwerkverbindung nicht absolut zuverlässig steht, kann es frustrierend sein, mit unterbrochenen Sitzungen zu kämpfen. Wie wir alle nur zu gut wissen, gibt es selbst in Hochgeschwindigkeitsnetzwerken einige Verzögerungen, wenn man auf dem einen Kontinent arbeitet und das Datencenter auf einem anderen Kontinent steht. Diese Probleme finden sich aber in jedem Szenario mit Remotezugriffen und es besteht kaum eine Gefahr, das ursprüngliche Dokument ungewollt zu beschädigen, indem man über eine langsame Verbindung in das Dokument schreibt. Eine getrennte Sitzung führt zu keinem Datenverlust – sie wartet lediglich darauf, dass sich der Benutzer erneut verbindet.

Wie lässt es sich realisieren, dass Benutzer vertrauliche Dokumente bearbeiten dürfen, wenn sie sich an einem sicheren Ort befinden, jedoch nicht, wenn sie auf das Firmennetzwerk vom örtlichen Internetcafé aus zugreifen möchten? Mit Terminaldiensten in Windows Server 2008 können Sie mithilfe von Regeln für den Remotezugriff festlegen, auf welche Anwendungen ein Remotebenutzer Zugriff hat, ob ihm lokale Laufwerke zugeordnet werden und sogar ob es möglich ist, Text zwischen lokalen und remoten Anwendungen auszuschneiden und einzufügen. Sicherheitserfordernisse können Einschränkungen für Remotezugriffe vorschreiben, wobei sich gleichzeitig dafür sorgen lässt, dass die Daten bei Bedarf leicht zugänglich sind.

Remotearbeit ermöglichen

Die Sicherheit für mobile Mitarbeiter steht in Zusammenhang mit dem allgemeinen Thema der Remotearbeit. Teleheimarbeit ist immer häufiger zu finden. Einige Helpdesk-Anbieter und US-Regierungsbehörden haben nicht einmal mehr Schreibtische für alle ihre Mitarbeiter, da die Arbeitsplätze so konzipiert sind, dass die meisten Personen überwiegend von zuhause aus arbeiten. Heimarbeit ist aber nicht nur ein nordamerikanisches Phänomen. Wie der Artikel »IT and the Environment« von Economist Intelligence Unit im November 2007 feststellt, arbeiten in 39 Prozent der westeuropäischen Firmen zumindest einige Mitarbeiter wenigstens einen Teil der Zeit zuhause.

Doch Heimarbeit bringt eigene Herausforderungen mit sich. Nicht zuletzt stellt sich die Frage, wie die Firma die Desktopumgebung unterstützen kann. Heimbasierte Computer lassen sich nicht ohne Weiteres durch Gruppenrichtlinien verwalten, sie können versagen, ohne dass IT-Personal unmittelbar helfend einschreiten kann, und Heimarbeiter können nicht immer ohne Weiteres über ein Computerproblem mit dem Personal vom Helpdesk sprechen. Und wie aktualisieren Sie eine Anwendung, wenn es an der Zeit ist, beispielsweise

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

von Microsoft Office 2003 auf Microsoft Office 2007 überzugehen? Wenn Sie wenigstens für einen kurzen Zeitraum unterwegs tätig waren, haben Sie wahrscheinlich die Vorteile der Mobilität und die Nachteile des fehlenden lokalen Supports kennen gelernt. Obwohl es großartig ist, vom Internetcafé oder der Lobby eines Flughafens aus zu arbeiten, ist es nicht allzu berauschend, als eigener Helpdesk zu fungieren. Serverbasierte Rechentechnik hilft auf verschiedene Art und Weise, Remoteszenarios zu ermöglichen. Als Administrator brauchen Sie sich keine Sorgen zu machen, dass Heimbenutzer Anwendungen installieren, die sie auf den Terminalservern nicht ausführen sollten, wenn Sie die grundlegenden Sicherheitsprozeduren (mehr zu diesem Thema später) befolgen. Da die Anwendungen auf den Terminalservern gespeichert sind, werden sie dort – und nicht auf den Clientcomputern – installiert und aktualisiert. Und wie bereits weiter vorn erwähnt, kann der Administrator durch die Terminaldienste bestimmen, wie die lokalen und remoten Computer die Ressourcen gemeinsam nutzen sollten und welche Anwendungen verfügbar sind, abhängig davon, woher ein Benutzer sich verbindet.

Windows auf PC-unfreundliche Umgebungen bringen

Obwohl der Schwerpunkt beim Client für Terminaldienste in Windows Server 2008 auf dem vollständigen Desktop liegt, ist die Möglichkeit, Windows Server 2008-ähnliche Fähigkeiten aus einem Computer herauszuholen, der Windows Server 2008 nicht ausführen kann, gegeben und hat ihre Anhänger. Ein Beispiel dafür sind Elektronikfirmen. Schaltkreise werden in einem so genannten *Reinraum* produziert, d.h. in einem Raum ohne Staub, bei dem es recht lange dauert, bis man durch verschiedene Schleusen eingetreten ist. Wenn Sie in einem Cleanroom auf Windows-Anwendungen angewiesen sind, kommen PCs nicht infrage, da deren Lüfter den Staub im Innern des Computers ansaugen und in den Raum blasen. Außerdem ist es nicht praktisch, PCs, die ständiger Wartung bedürfen, an Orten wie eben einem Cleanroom einzusetzen, wo für das Betreten umfangreiche Vorbereitungen notwendig sind. Demzufolge brauchen Sie Terminaldienste, um Windows-Anwendungen für die Terminals bereitzustellen.

Thin Clients eignen sich ebenfalls gut für Umgebungen, in denen Sie auf Windows-Anwendungen zugreifen möchten, wo aber die Umstände eher PC-feindlich sind – sie bekommen zu viel Staub oder Erschütterungen ab, die ein PC nicht verträgt. Kleine Terminals, die sich an der Wand montieren lassen oder portabel sind, arbeiten besser unter diesen Umständen als PCs. Diese kleinen Terminals müssen jedoch mit recht wenig Arbeitsspeicher, geringer Rechenleistung und ohne Festplatte auskommen, sodass Sie darauf auch kein Windows Vista betreiben können. Um auf das neueste Betriebssystem und die neuesten Anwendungen zugreifen zu können, brauchen Sie einen Terminalserver, an dem die Terminals angeschlossen sind.

PC-lose Windows-Umgebungen finden sich an Orten wie zum Beispiel besseren Fitnessstudios oder in den Foyers von Stadtwohnungskomplexen. Das Management möchte Kunden anziehen, indem es die Annehmlichkeiten eines Personalcomputers im Foyer oder Café bietet, aber an diesen Plätzen keine Computer unterstützen möchte. Der Raumbedarf kann ebenfalls ein Punkt sein, wenn Sie versuchen, fünf Benutzerarbeitsbereiche an einem kleinen Schalterraum zusammenzuquetschen. Windows-Terminals können sich mit einem Terminalserver verbinden und die Anwendungen präsentieren; abgesehen davon sind sie kleiner, cooler und zuverlässiger als PCs, die möglicherweise noch falsch konfiguriert werden.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

Gelegentlich hört man, dass es keinen Grund gibt, Thin Clients anzuschaffen, da man für dasselbe Geld PCs mit mehr Leistung bekommt. Bei Thin Clients bezahlen Sie nicht für die Rechenleistung – tatsächlich verwenden Sie vergleichsweise recht wenig. Sie bezahlen für die reduzierte Administration und den geringeren Energiebedarf. Diese Lösung ist nicht für die Allgemeinheit geeignet, doch manchmal sind Thin Clients einfach eine bessere Wahl als PCs.

Umweltfreundliche EDV unterstützen

Zu den heißen Themen dieser Tage (kein beabsichtigtes Wortspiel) gehört es, wie sich Firmen und Behörden grüner machen lassen – wie ihnen dabei geholfen wird, Energie einzusparen. Das Marktforschungsinstitut IDC stellt fest, dass der Energieverbrauch heutzutage eines der fünf wichtigsten Anliegen von Systemmanagern ist. Unternehmen verbrauchen bisher rund zehn Prozent ihres Technologiebudgets für Energie, sagt Rakesh Kumar von der Beraterfirma Gartner. Nur etwa die Hälfte davon wird für den Betrieb der Computer benötigt; einen Großteil verbraucht die Kühlung, da für jeden Dollar, der in den Strom eines Servers fließt, ein Doller für Kühlung aufzuwenden ist. Das Senken des Energieverbrauchs ist in der Tat eine Win-Win-Situation – da Firmen für ihre Energie bezahlen, bedeutet ein geringerer Energieverbrauch, dass sie weniger Geld in Energie investieren müssen.

HINWEIS Der Artikel »Reducing U.S. Greenhouse Gas Emissions: How Much at What Cost?« (*http://www.mckinsey.com/clientservice/ccsi/pdf/US_ghg_final_report.pdf*) von McKinsey & Company (Dezember 2007) zeigt die marginalen Kosten für die Reduzierung der Kohlendioxidemission auf. Rechnet man diese Kosten mit denen für Heizung und Strom in Geschäftsgebäuden zusammen, ergibt sich ein negativer Wert. Das heißt, es zahlt sich für die Firmen aus, den grünen Weg einzuschlagen.

In desktoporientierter EDV gibt es Verschwendung *in Größenordnung*. Laut IDC reicht der Nutzungsgrad bei Servern von 15 bis 30 Prozent. Durchschnittliche Ressourcennutzungsraten für PCs werden mit weniger als 5 Prozent geschätzt. Da Prozessor und Speicher mit Strom zu versorgen sind, ob sie nun verwendet werden oder nicht, bedeutet dies Verschwendung im großen Stil. Demzufolge gibt es je nach den Anforderungen des Clients ziemlich viel Raum für Benutzer, die auf ihre Desktops oder zumindest auf ihre Anwendungen von einem Terminalserver aus zugreifen. Für Unternehmen, die Desktopcomputer in zweckmäßiger Form durch Windows-basierte Terminals austauschen können, bietet das ein riesiges Einsparungspotenzial sowohl in Bezug auf den Energieverbrauch voll ausgerüsteter Desktops als auch in Bezug auf die Klimatisierung des Gebäudes, das von Hunderten leistungsstarker PCs aufgeheizt wird.

Terminaldienste für Windows Server 2008: Das Gesamtbild

Die letzten Abschnitte haben einige Möglichkeiten dargestellt, wie Sie serverbasierte EDV anwenden können, um den Anforderungen eines Unternehmens für mobile Benutzer oder PC-feindliche Umgebungen zu entsprechen. Viele neue Features in Windows Server 2008 helfen dabei, speziell diese Szenarios zu unterstützen. Dieses Buch soll Ihnen vermitteln, was in Terminaldiensten neu ist und wie sie zu verwenden sind. Dieser Abschnitt beschäftigt sich nun mit einigen der Features und wie sich diese Version der Terminaldienste gegenüber vorherigen unterscheidet, und zwar in einem größeren Rahmen als ihre Features für sich genommen.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

Der sich ändernde Charakter der Terminalservernutzung

Zu den Änderungen bei Terminaldiensten in Windows Server 2008 gehören die Annahmen über das Nutzungsverhalten. Zum Beispiel geht Windows Server 2003 davon aus, dass Administratoren im Allgemeinen einzelne Server vom lokalen Netzwerk (LAN) der Firma aus betreiben und wahrscheinlich auch nur einen oder zwei davon, da die Sitzungsbrokerkomponente nur in der Enterprise Edition verfügbar ist. Die in Windows Server 2008 vorhandenen Features nehmen Folgendes an:

- Viele Endbenutzer greifen auf das Firmen-LAN zumindest zeitweise über das Internet zu.
- Endbenutzer melden sich nicht immer von Computern an, die zur Domäne gehören.
- Endbenutzer führen eher einen vollständigen Desktop aus (mit einigen lokal installierten Anwendungen) aus als ein Terminalgerät.
- Endbenutzer können von einer Zweigstelle aus arbeiten, sind aber trotzdem noch mit der Domäne verbunden.
- Administratoren brauchen mehr Kapazität für das Bedienen von Anwendungen als einen einzelnen Server – sie müssen in der Lage sein, eine gewisse Redundanz einzubauen.

Wir führen hier einige Rollendienste für Terminaldienste ein, doch ist im Augenblick weniger wichtig, diese Features vom technischen Hintergrund aus zu betrachten, als die Geschäftsprobleme zu erfassen, für deren Lösung sie konzipiert sind.

Telearbeiter und mobile Benutzer unterstützen

In den letzten Jahren hat sich in der IT-Branche im Hinblick auf den Arbeitsstil ein großer Wandel vollzogen. Einst sind die meisten Beschäftigten in der Informationsverarbeitung (so lassen sich am besten die Leute beschreiben, die regelmäßig auf einen gemeinsamen Datenpool zugreifen, um ihre Jobs zu erledigen) dorthin gegangen, wo die Informationen waren: ins Büro. Der Arbeitsschluss markierte auch das Ende der Arbeiten an all dem, was von diesem zentralen Informationspool abhängig war. Im Büro konnten sie leicht zu diesem zentralen Informationspool beitragen – immerhin wurden alle diese Informationen von den Mitarbeitern erzeugt – und wenn sie gingen, konnten sie auch nichts mehr zum zentralen Informationspool beisteuern.

Laptops haben dieses Bild geändert. Telecommuter hatten einen Computer, den sie problemlos bei sich tragen konnten, doch hatten Laptops immer noch keinen Zugriff auf den zentralen Informationspool, der den Mitarbeitern im Büro zugänglich war. Weitverbreiteter Internetzugriff kombiniert mit der zunehmenden Nutzung von E-Mail als persönlichem Informationsspeicher verbesserte zwar die Lage, doch bieten die E-Mail-Funktionen nicht alles das, was das Unternehmen weiß – es stehen nur die Informationen zur Verfügung, die in den gesendeten oder empfangenen E-Mails eingebunden sind.

In der nächsten Stufe ließen sich gesicherte Verbindungen zum Firmennetzwerk herstellen, Informationen je nach Bedarf abrufen und dann auf den Laptop herunterladen. Natürlich verlangte das breiten Zugriff auf Hochgeschwindigkeitsnetzwerke für das Herunterladen von Dokumenten auf den lokalen Computer wie auch für die lokal zu installierenden Anwendungen. Das bedeutete auch, dass die Mitarbeiter eine Möglichkeit für den Laptop brauchten, um auf das Datencenter zuzugreifen, ohne die Sicherheit zu verletzen oder einen Virus in das Firmennetz einzuschleusen.

Ein großer Teil der heutigen industrialisierten Welt hat Zugriff auf die erforderlichen Komponenten: Laptops und Hochgeschwindigkeitsnetzwerke, die sowohl zuhause als auch an öffentlichen Orten wie Flughäfen und Hotels vorhanden sind. Daraus erwachsen aber auch komplexe Probleme. So stellt sich die Frage,

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

welche Computer auf das Netzwerk zugreifen dürfen und wie sich vertrauliche Daten von Computern fernhalten können, die durch Diebstahl oder Verlust gefährdet sind. Außerdem ist zu klären, wie sich die Daten zugänglich machen lassen, die mobile Mitarbeiter unterwegs erzeugen. Diese Daten finden erst ihren Weg zurück in das Firmennetz, wenn die Straßenkämpfer von ihrem Ausflug zurückkommen oder wenigstens etwas freie Zeit erübrigen, um alle ihre neuen Daten in den zentralen Datenpool hochzuladen.

Terminaldienste haben lange Zeit versprochen, Telecommuter und mobile Arbeiter zu unterstützen, doch brachte die in das Betriebssystem integrierte Lösung nicht alle erforderlichen Tools mit, damit dies funktioniert. Windows Server 2008 hat dies mit der Einführung von Terminaldienstegateway geändert. Dieser Rollendienst versetzt Benutzer in die Lage, sicher auf das Firmennetzwerk – und den zentralen Datenpool – über HTTP Secure Sockets Layer (SSL oder HTTPS) vom Hotel oder Flughafen aus zuzugreifen (vielleicht auch vom Strand aus, wenn Sie wissen, wie Sie den Sand wieder aus dem Laptop bekommen). In Kombination mit RDP-Dateisignierung und Serverauthentifizierung bietet Terminaldienstegateway einen geschützten Internetzugriff, sodass Endbenutzer relativ sicher sein können, dass die in einer E-Mail erhaltene RDP-Datei eine legitime Ressource darstellt und kein gespooftes Serversetup ihre Anmeldeinformationen abfangen kann.

HINWEIS Terminaldienstegateway und SSL sind nicht die einzigen Methoden, um eine sichere Verbindung zum Datencenter von einem Remotestandort herzustellen – virtuelle private Netzwerke (VPNs) kommen ebenfalls infrage. Doch besitzt Terminaldienstegateway bestimmte Vorteile gegenüber VPNs. Dazu gehört der granulare Zugriff auf Ressourcen, mit dem sich Kapitel 7 ausführlich beschäftigt.

Öffentliche Computer verwenden

Der vorherige Abschnitt hat erläutert, dass die meisten Benutzer mit ihren persönlichen Laptops arbeiten. Allerdings ist es nicht vernünftig zu erwarten, dass sich Benutzer ausschließlich von einem Computer aus anmelden, dessen Besitzer sie sind. Zum Beispiel können Sie sich an den Terminalservern der Firma von einem Computer aus anmelden, der bei Ihnen zuhause in Tucson steht, oder von einem Kiosk in einem Internetcafé in Darmstadt. In beiden Fällen brauchen Sie eine Möglichkeit, um auf Arbeitsressourcen zuzugreifen, ohne irgendwelche persönlichen Daten in den Caches dieser Computer zurückzulassen. Terminaldienste-Webzugriff besitzt Features, mit denen Sie dies realisieren können.

Integrierter Desktop und remote Arbeitsbereiche

Terminaldienste in Windows Server 2008 verlangen kein spezifisches Clientbetriebssystem – die Verbindung können Sie mit Clients bis zurück zu RDP 5.2 herstellen. (Aufgrund von Sicherheitsverbesserungen in RDP 5.x werden vorherige Versionen von RDP nicht unterstützt.) Abgesehen davon besteht in dieser Version von Windows Server 2008 eine neue gegenseitige Abhängigkeit zwischen Client und Server bei der Unterstützung der Mehrbenutzererfahrung. Die neuen Szenarios, die Windows Server 2008 erlaubt, wie zum Beispiel das Feature für einmaliges Anmelden (Single Sign-On, SSO) und RemoteApp-Programme, verlangen die neueste Version des RDP-Clients (6.1), die nur von Windows Vista SP1 und Windows XP SP3 unterstützt wird. Damit wird angestrebt, Terminaldienste zu einer Erweiterung des Windows-Desktops zu machen, d.h. nicht vollständig zu ersetzen (und damit anzuerkennen, dass dies im Allgemeinen der Fall gewesen ist, seit Windows-Terminaldienste eingeführt wurden). Terminaldienste in Windows Server 2008 verwischen die Grenze zwischen Desktop und Terminalserver.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

Von Zweigstellen aus arbeiten

Remote arbeiten ist nicht nur eine Bezeichnung für diejenigen, die von zuhause oder von unterwegs aus arbeiten. Remotearbeiter können auch in einem eigenen Büro sitzen – aber in einem Büro, das vergleichbare Ressourcen wie das Firmenbüro bietet. In diesem Szenario ist das Netzwerk zuverlässig, die Computer sind in die Domäne eingebunden – das Datencenter befindet sich aber nicht am selben physischen Standort wie die Zweigstelle und vor Ort sind nur wenige IT-Mitarbeiter tätig.

Große Serverfarmen

Terminalserver-Bereitstellungen bestehen nicht mehr nur aus einem oder zwei Servern, doch die Tools in Windows Server 2003 haben große Farmen nicht wirklich unterstützt. (Sitzungsverzeichnisserver waren nur in der Enterprise Edition verfügbar.) Windows Server 2008-Terminaldienste eignen sich besser, um Zugriff auf mehrere Server zu verwalten, weil es durch zusätzliche Gruppenrichtlinien für die Serververwaltung und den verbesserten Sitzungsbroker in der Standardedition von Windows Server 2008 möglich ist, dass sich Endbenutzer mit Farmen verbinden können, anstatt konkrete Server angeben zu müssen.

Aus erster Hand: Andere Geschäftsszenarios für Terminaldienste

Administratoren profitieren ebenfalls von Terminaldiensten.

Einhaltung behördlicher Vorschriften

Für die IT-Abteilung haben Datensicherheit und die Möglichkeit, gesetzliche Anforderungen zu erfüllen, immer höchste Priorität. Terminaldienste helfen dabei, eine Anwendung und ihre Daten an einer zentralen Stelle zu sichern, was das Risiko eines unvorhersehbaren Datenverlustes – beispielsweise durch Diebstahl eines Laptops – verringert. Mit den Hauptfeatures der Terminaldienste wie zum Beispiel Terminaldienstegateway und Terminaldienste-RemoteApp lässt sich gewährleisten, dass Partner – oder Benutzer –, die keinen vollen Zugriff auf das Netzwerk oder die Computer einer Firma benötigen, bei Bedarf auf eine einzige Anwendung eingeschränkt werden können.

Komplexe Anwendungen

In einer Umgebung mit komplexen Anwendungen (wie zum Beispiel Branchensoftware oder angepasster Legacysoftware) oder in Situationen, in denen große und komplexe Anwendungen häufig zu aktualisieren sind, was sich aber nur schwer automatisieren lässt, können Terminaldienste helfen, den Prozess zu vereinfachen, indem sie die Belastung, die bei Ausführung mehrerer Anwendungen entsteht, auf die gesamte Umgebung verteilen. Die Clientcomputer können auf die für sie benötigten Anwendungen von einer zentralen Quelle aus zugreifen, anstatt die Anwendungen lokal installieren zu müssen.

Integration bei Fusionierung oder Outsourcing

Bei einer Fusion müssen die betroffenen Organisationen in der Regel die gleichen Branchenanwendungen einsetzen, obwohl sie in den verschiedensten Konfigurationen und Versionen vorliegen. Außerdem werden Organisationen mit ausgegliederten oder Partnerorganisationen zusammenarbeiten, die zwar Zugriff auf spezifische Branchenanwendungen, aber nicht auf das komplette Firmennetzwerk benötigen. Anstatt eine kostspielige Bereitstellung aller Branchenanwendungen über die erweiterte Infrastruktur vorzunehmen, lassen sich diese Anwendungen auf einem Terminalserver installieren und für die Mitarbeiter und Geschäftspartner zugänglich machen, die dann im Bedarfsfall darauf zugreifen können.

Alex Balcanquall

Product Manager

Attraktive Neuerungen für Terminaldienste in Windows Server 2008

Neue Features der Terminaldienste in Windows Server 2008 tragen eine Menge zur Verbesserung der Benutzerfreundlichkeit bei. Fat Clients sind ausgesprochen leistungsfähig geworden, wenn es um Anzeige- und Desktop Experience-Funktionen geht, und serverbasierte EDV muss in dieser Beziehung mithalten.

Den wirklichen Überblick mit Unterstützung für mehrere Monitore verschaffen

Die Windows Server 2003-Anzeige sieht recht ansprechend aus. Bei einer maximalen Anzeigegröße von 1600 x 1200, Unterstützung für 32-Bit-Farben und zugeordneten Laufwerken stellt dies eine große Verbesserung gegenüber Windows 2000 Server dar. Inzwischen aber haben sich viele Benutzer an mehrere Monitore und clientseitige Hardware gewöhnt, die vor fünf Jahren noch nicht üblich war. Remotebenutzer können sich per RDP 6.1 mit einem Windows Server 2008-Terminalserver verbinden und eine Anzeige nutzen, wie sie sie schon vom lokalen Computer her gewohnt sind. Dazu gehören:

- Unterstützung für mehrere Monitore mit der gleichen Auflösung und nebeneinander stehend ausgerichtet
- Unterstützung für benutzerdefinierte Anzeigeauflösungen
- Unterstützung für Großbildschirme (bis zu 4096 x 2048)

HINWEIS Leider unterstützen Terminaldienste in Windows Server 2008 nicht die Ansicht Aero-Glas von Windows Vista.

Kapitel 4 geht ausführlicher darauf ein, wie Sie die Anzeigeeinstellungen für Clients konfigurieren und welche Dinge zu beachten sind, wenn Sie die Unterstützung für mehrere Monitore aktivieren.

Breitere Unterstützung für clientseitige Geräteumleitung

Bei Einführung der Terminaldienste waren auf der Clientseite in erster Linie die Geräte Tastatur und Maus zu unterstützen. Als Nächstes kam die Forderung für Drucker hinzu, damit Endbenutzer Dokumente auf einem Drucker ausgeben konnten, der am Client angeschlossen war. Lokale Laufwerke rückten auf der Prioritätenliste nach oben, damit Endbenutzer Dateien von und auf ihre lokalen Laufwerke kopieren und bei Bedarf sogar Dateien von Anfang an lokal speichern konnten.

In heutigen Arbeitsumgebungen sind sogar noch mehr Geräte zu unterstützen. Zwei wichtige Konsumentengeräte sind Mediaplayer und Digitalkameras. Wenn Sie in einer vollkommen remoten Umgebung arbeiten, müssen Sie diese Geräte von der Remotesitzung aus steuern und Daten zu und von den Remotegeräten kopieren können. Mithilfe von Windows Server 2008-Terminaldienste mit Remote Desktop Client (RDC) 6.1 lassen sich Geräte zuordnen, die das Media Transfer-Protokoll (MTP) für Mediaplayer verwenden, und Digitalkameras, die mit dem Picture Transfer Protocol (PTP) arbeiten. Consumergeräte stehen im Hinblick auf erforderliche Unterstützung aber nicht allein. In Windows Server 2008 ist die Unterstützung für clientseitige POS (Point Of Service)-Geräte ebenso für Einzelhändler verfügbar. Mit der Unterstützung und der Konfiguration der clientseitigen Geräteumleitung beschäftigen wir uns eingehend in Kapitel 5.

HINWEIS Unterstützung für POS-Umleitung verlangt, dass der Server ein x86-Computer ist und die Geräte mit .NET Framework 1.1 oder später arbeiten.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

Aus erster Hand: Warum Plug & Play?

Plug & Play-Geräte sind heutzutage in Windows die Norm. Das bedeutet, dass lokal angeschlossene Plug & Play-Geräte nahtlos in Remotesitzungen arbeiten sollten. Wir haben eine Infrastrukturkomponente namens *Terminal Server Plug and Play Device Redirection Framework* eingeführt, die Ihnen dabei hilft, alle diese lokal angeschlossenen Plug & Play-Geräte umzuleiten, die noch nicht von vorhandenen Geräteumleitungen in der Welt der Terminaldienste abgedeckt sind. Das Framework erlaubt in Verbindung mit einfachen Richtlinien für Programmierer von Plug & Play-Gerätetreibern, die im Rahmen des Logo-Programms von Windows Vista und Windows Server 2008 veröffentlicht werden, jedem Plug & Play-Gerät von Drittanbietern in Remotesitzungen verfügbar zu sein, wenn die Gerätetreiber ordnungsgemäß programmiert sind.

Als Nachweis der Machbarkeit haben wir uns dafür entschieden, Kernunterstützung für zwei Klassen von Geräten bereitzustellen: Tragbare Geräte (MTP-basierte Fotokameras und Mediaplayer) und POS (Point Of Service)-Geräte, die auf dem Microsoft POS-Stack für .NET Framework 1.1 aufbauen. Als entscheidender Punkt ist hier anzumerken, dass dieses Feature Umleitung für alle mit den Logo-Richtlinien kompatiblen Plug & Play-Geräte bietet, und zwar unabhängig von ihren Verbindungsmechanismen – es handelt sich also nicht einfach um eine USB (Universal Serial Bus)-Geräteumleitung.

Gaurav Daga

Program Manager

Einmaliges Anmelden

Einmaliges Anmelden bedeutet für den Endbenutzer, dass er das Kennwort nur einmal eingeben muss, um auf die Ressourcen des Computers zugreifen zu können – eine zweifellos komfortable Angelegenheit. Stellen Sie sich vor, dass Sie morgens ins Büro kommen und sich an Ihrem Computer anmelden. Dann klicken Sie auf ein Symbol und müssen die Anmeldeinformationen erneut eingeben. Beim Klicken auf ein anderes Symbol werden wieder die Anmeldinformationen verlangt. Gegen 10 Uhr sind Sie wahrscheinlich drauf und dran, erstmal eine Kaffeepause einzulegen. Zweifellos ist es der Produktivität nicht zuträglich, sich bei jedem Starten einer Anwendung anmelden zu müssen.

Genau dies könnte mit Terminaldiensten ohne das Feature *einmaliges Anmelden* (Single Sign-On, SSO) passieren. Sie kommen am Morgen zur Arbeit und melden sich an Ihrem Computer an, müssen sich aber beim Terminalserver authentifizieren, um Remoteanwendungen nutzen zu dürfen. Jedes Mal, wenn Sie sich mit einem Terminalserver verbinden, müssen Sie sich selbst erneut authentifizieren. Bei einer Verbindung über das Internet müssen Sie beim Gateway-Server authentifiziert werden, der steuert, wer von außerhalb des Firmen-LAN die Terminalserver verwenden darf.

Um zu vermeiden, dass Sie den ganzen Tag damit verbringen, sich anzumelden oder eine Delle in Ihre Tastatur einzuarbeiten, wenn Sie mit Ihrem Kopf auf dem Schreibtisch aufschlagen, brauchen Sie einen Mechanismus, um sich einmalig anzumelden und dann keinen Gedanken mehr daran verschwenden zu müssen. Zum Glück haben Sie einen: Windows Server 2008 unterstützt einmaliges Anmelden, um Anmeldeinformationen von Windows Vista- oder Windows XP SP3-Clients, die Mitglied der Domäne sind, zu übergeben. Müssen Sie Ihre Anmeldeinformationen an einem Terminalserver präsentieren, wird dies automatisch für Sie erledigt. Kapitel 7 erläutert, wie Sie dies einrichten.

Druckertreiber eliminieren

Druckertreiber sind lange Zeit der Fluch für den Administrator von Terminaldiensten gewesen. Zunächst einmal war die Unterstützung von Druckertreibern ein Spiel, in dem Sie gewonnen hätten, wenn der Treiber den Terminalserver nicht zum Absturz gebracht hätte. Durch die Unterstützung clientseitiger Drucker wurde das System zunehmend für fehleranfällige Treiber geöffnet, da die Kontrolle des Administrators über die installierten Treiber geschwächt wurde. Werden Windows NT-Treiber auf den Terminalservern und Nicht-Windows NT-Treiber auf dem Client unterstützt (wenn man beispielsweise Windows 98 als Client für einen Terminalserver unter Windows 2000 Server einsetzt), haben die Treiber unter Umständen verschiedene Namen. Der Administrator müsste dann Treiberzuordnungsdateien erstellen, die prinzipiell sagen: »Wenn das System auf diesen Treiber aus der Clientsitzung heraus verweist, ist jener Treiber auf dem Terminalserver zu verwenden.« Andernfalls würde der Druckauftrag nicht ausgeführt.

Da man mit der Zeit das Problem besser verstanden hat, sind die Treiber auch zuverlässiger geworden. Und wenn sowohl Client als auch Terminalserver auf Windows NT-Technologie aufbauten, hörte das Problem der nicht übereinstimmenden Treibernamen auf zu existieren. Windows Server 2003 führte dann eine neue Gruppenrichtlinie ein, die standardmäßig nur Benutzermodustreiber erlaubte. Damit verschwand das Risiko, schlecht geschriebene Kernelmodustreiber zu installieren, die den Server zum Absturz bringen, doch bedeutete es weiterhin, dass Terminalserveradministratoren eine ganze Palette von Treibern sowohl für die Drucker der Firma als auch die zugeordneten Clientdrucker testen, verwalten und unterstützen mussten (auch wenn manche Firmen die Unterstützung von untergeordneten Clientdruckern gestoppt haben, allein um Treiberprobleme zu vermeiden).

Hinter den Kulissen: Warum spielt es eine Rolle, ob Treiber für den Benutzermodus oder den Kernelmodus geschrieben sind?

Wenn es Ihnen nicht gleich einleuchtet, warum eine Richtlinie, die nur Benutzermodustreiber erlaubt, notwendig oder wünschenswert sein könnte, lesen Sie weiter.

Jede Komponente des Windows-Betriebssystems ist dafür konzipiert, Speicher von einem bestimmten Abschnitt des Speichers anzufordern, der in Blöcken organisiert ist. Der Umfang des Speichers, auf den ein Betriebssystem zugreifen kann, hängt vom unterstützten Adressierungsschema ab. Zum Beispiel können 32-Bit-Betriebssysteme lediglich bis zu 4 GB Speicher ansprechen und dieser Speicher ist normalerweise in zwei Teile gegliedert: die oberen 2 GB Speicher für den Kernelmodus und die unteren 2 GB für den Benutzermodus. Die Kernelmoduskomponenten haben Zugriff auf die eigentlichen physischen Speicherstrukturen. Benutzermoduskomponenten können nur auf eine zugeordnete Ansicht dieser Strukturen zugreifen.

Es verhält sich so, als ob die Speicherstrukturen einen Satz von innerbetrieblichen Briefkästen darstellen. Die Komponenten des Kernelmodus haben Zugriff auf die Briefkästen selbst – die Kästen, die körperlich an der Wand aufgereiht sind. Benutzermoduskomponenten können nicht auf die Kästen zugreifen. Stattdessen zeigen sie an, dass ein Datenelement in den Kasten gehen sollte, der zu Kim Abercrombie oder zu Michael Pfeiffer gehört. Die Kernelmoduskomponente erstellt die Zuordnung, die angibt, welche physische Speicherstelle mit Kim Abercrombie verbunden ist, und leitet die Daten dorthin weiter. Somit landen die Daten auch dann an der richtigen Stelle, wenn die Kästen vertauscht werden oder Kim ein neues Postfach erhält. Ähnlich sieht es aus, wenn eine Benutzermoduskomponente Daten von einer bestimmten Speicherstelle benötigt, von der die Komponente den physischen Speicherplatz der Daten nicht kennt, aber ihn ▶

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

entsprechend ihren virtuellen Daten anspricht – »Ich brauche die Daten, die im Briefkasten von Kim Abercrombie gespeichert sind.« Die Kernelmoduskomponente ordnet dann den Namen von Kim Abercrombie einem Briefkastenstandort zu und ruft die Daten ab. Der Bereich des Speichers, für den eine Komponente konzipiert ist, hängt davon ab, was diese Komponente tun muss, wie schnell sie es tun muss und wie wahrscheinlich es ist, dass dabei ein Problem auftritt. Fast alle Vorgänge, die man in einem Computer wahrnimmt, finden im Benutzermodus statt: Anwendungen öffnen, Fenster verschieben, Zeichen auf dem Monitor darstellen, wenn sie eingegeben werden, usw. Operationen, die im Benutzermodus laufen, sind gegeneinander geschützt, da sie in virtuelle und nicht in physische Speicherstellen schreiben. Kernelmoduskomponenten stellen sicher, dass diese Operationen nicht an dieselben physischen Speicherstellen schreiben. Aus diesem Grund wird der Benutzermodus auch als *geschützter Modus* (*Protected Mode*) bezeichnet. Stürzt eine Anwendung ab, die im Benutzermodus läuft, beeinflusst sie keine anderen Anwendungen.

Komponenten im Kernelmodus sind etwas schneller als Benutzermoduskomponenten, da sie keine virtuellen Speicheradressen in physische Adressen übersetzen müssen. Allerdings sind sie anfälliger für Fehler. (In diesem Kontext macht *etwas schneller* keinen Unterschied, den Sie als Administrator oder Endbenutzer bemerken.) Kernelmodus verweist auf die physischen Speicherstrukturen, die von allen Komponenten auf demselben Computer gemeinsam genutzt werden. So kann es durchaus vorkommen, dass zwei Anwendungen versuchen, Informationen im selben Speicherbereich abzulegen. Wenn dies passiert, stürzen die Komponenten ab und können sogar das gesamte Betriebssystem mit zu Boden reißen. Demzufolge gefährden Druckertreiber, die im Kernelmodus auf einem Terminalserver laufen, nicht nur den Arbeitsbereich eines Benutzers, sondern die Arbeitsbereiche aller Benutzer auf demselben Computer. Auch wenn Druckertreiber auf Terminalservern heute wesentlich zuverlässiger arbeiten, ist es besser, nur Benutzermodustreiber zu verwenden. Wenn Sie unbedingt auf Kernelmodustreiber angewiesen sind, müssen Sie sie testen, bevor Sie sie in die Produktion überführen.

Aus technischer Sicht arbeiten die Benutzermodustreiber nur teilweise im Benutzermodus oder sind zumindest nicht in der Lage, alle ihre Aufgaben aus dem Benutzermodus heraus durchzuführen. Sie kommunizieren immer noch mit einer Kernelmoduskomponente, die die Daten an dem physischen Speicherort ablegt, wo sie hingehören. Wenn jedoch der Benutzermodusteil scheitert, beeinflusst dies nicht den Kernelmodusbereich des Speichers.

Das Speicherlayout ist für Terminalserver immens wichtig und in Kapitel 2 gehen wir ausführlich darauf ein.

Problematisch bei vorherigen Druckkonzepten war die Entscheidung, welche Drucker der Remotesitzung zugeordnet werden sollten. Bei aktivierter Druckerzuordnung werden alle Clientdrucker dem Terminalserver zugeordnet, unabhängig davon, ob dies zweckmäßig ist oder nicht. Das Zuordnen aller dieser Drucker konnte ziemlich zeitaufwändig sein, ganz zu schweigen von der erhöhten Anzahl der Treiber, die auf einem Terminalserver installiert sein mussten.

Terminaldienste in Windows Server 2008 begegnen diesen Problemen mit verschiedenen Methoden. Bei der ersten (und einfachsten) Methode erlaubt eine Gruppenrichtlinie den Administratoren, nur die Standarddrucker des Clients zu einer Terminalsitzung zuzuordnen. Zweitens vermeidet die Easy Print-Technologie das Treiberproblem für Windows Vista-Clients, die Remotedesktopverbindung 6.1 ausführen. Prinzipiell erlaubt Easy Print den Endbenutzern, von einer Remotesitzung aus zu drucken, ohne überhaupt irgendwelche Treiber auf der Terminalsitzung zu installieren. Die Remotesitzung erhält die Druckereinstellungen vom Clientcomputer und führt sogar Aufrufe zur clientseitigen GUI aus, um die Treiberkonfigurationsfenster für die Treiber anzuzeigen.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

In Kapitel 5 erfahren Sie mehr zur Funktionsweise von Easy Print und wie Sie Ihr System konfigurieren, um dieses Feature zu verwenden oder zu deaktivieren.

Aus der Praxis: Easy Print ist einfach

Unabhängig davon, wie Benutzer traditionell ihre Anwendungen bekamen – das Thema Drucken und Druckertreiber war lange Zeit der Fluch der Terminaldienste-Administratoren. Die Entscheidung, die richtigen Treiber auf den richtigen Servern unterzubringen – und zu hoffen und zu beten, dass keiner von ihnen einen der gefürchteten STOP-Fehler (Bluescreen) verursachte – hat manchem Administrator schlaflose Nächte bereitet. Mit vorherigen Versionen der Terminaldienste war es entscheidend, dass der Gerätetreiber auf dem Server mit dem Treiber, der auf dem Client installiert war, übereinstimmte. Mit den überall umherschwirrenden Treibernamen endete es oft mit einem Fehler, wenn man diese 1:1-Zuordnung sicherstellen wollte.

Mit Windows Vista und Windows Server 2008 ist ein großer Teil dieser Qual verschwunden. In den Terminaldiensten von Windows Server 2008 braucht der Administrator keine Treiber mehr auf dem Terminalserver zu installieren. Diese Funktionalität wird mit dem XPS-Druckpfad realisiert, der in Windows Vista eingebunden ist. Dieser Druckpfad bedeutet in Verbindung mit der Fähigkeit, den Drucker nach unten zum Client umzuleiten, dass der Benutzer seine lokalen Druckertreiber nutzen kann, um auf Remotedruckern zu drucken. Da der XPS-Druckpfad standardmäßig auf jedem Vista-Client vorhanden ist, können Druckaufträge mit einem Maximum an Vertrauen, dass sie mithilfe des Clienttreibers akkurat drucken, umgeleitet werden.

Wie sieht dies für den Client aus? Wenn ein Client mit Windows Vista eine Verbindung zu einem Windows Server 2008-Terminalserver herstellt und klickt, um die Druckereigenschaften anzuzeigen, erscheint die gleiche Benutzeroberfläche für Druckereigenschaften, die er schon immer bei seinem lokalen Druckertreiber gesehen hat. Tatsächlich wird die Benutzeroberfläche, mit der der Benutzer diesen Drucker konfiguriert, auf dem Clientcomputer ausgeführt. Beim Klicken auf *Drucken* wird ein XPS-Druckauftrag auf dem Server erstellt, der an den Client zurückgeschickt und über die lokale Verbindung gedruckt wird.

Offenbar gibt es nun einige Umgebungen, in denen dies nicht die optimale Konfiguration darstellt. Wenn der Druckerserver in Netzwerknähe zum Terminalserver statt zum Client ist, muss dieser Auftrag das Netzwerk praktisch zweimal durchlaufen. Citrix bringt für derartige Szenarios einen Mechanismus mit, um lokales Drucken auf dem Citrix-Server zu konfigurieren. Für die meisten Konfigurationen befindet sich der Drucker aber unmittelbar neben dem Client und entfernt vom Terminalserver. Deshalb dürften die meisten Benutzer dieses neue Feature schätzen.

Greg Shields, MCSE: Security, CCEA

»On the Server Side of Terminal Services«, MCP Magazine, Januar 2008

Mit freundlicher Genehmigung

Terminaldienste-RemoteApp

Als Letztes der neuen Features für Benutzerfreundlichkeit sei hier RemoteApp erwähnt. Historisch sind native Terminaldienste eine Methode gewesen, einen vollständigen Desktop und nicht nur einzelne Anwendungen »fernzusteuern«. Beim Remotezugriff auf einen Desktop werden überflüssige Symbole vom Desktop entfernt, um die Benutzer nicht zu verwirren oder abzulenken. Die in der Remotesitzung laufenden Anwendungen sind also nicht besonders gut mit den lokal ausgeführten Anwendungen verzahnt und der Endbenutzer muss sich merken, ob eine Anwendung lokal oder remote ausgeführt wird.

In vorherigen Versionen von Terminalserver war es möglich, eine RDP-Datei nur auf eine einzelne Anwendung verweisen zu lassen, wobei die Remotesitzung beendet wurde, wenn der Endbenutzer die Anwendung geschlossen hat. Dieses Konzept hatte in der Praxis mehrere Nachteile:

- Die Anwendung lief in einem Frame für eine Remotesitzung und sah nicht wie eine lokal laufende Anwendung aus.
- Das Symbol der Anwendung in der Taskleiste stand für eine Remotesitzung und nicht für die Anwendung selbst. Haben Benutzer mehrere Anwendungen auf diese Weise ausgeführt, konnten sie sie nicht mehr auseinander halten, wenn die Anwendungsfenster minimiert waren.
- Jede Anwendung zeigte ihre eigene Sitzung auf diese Weise an. Der Terminalserver musste also eine komplette Sitzung für jede einzelne in dieser Form präsentierte Anwendung verwalten, wodurch sich der Speicheroverhead vergrößerte. Außerdem hieß das, dass jede so geöffnete Anwendung eine eigene Kopie des Terminalserverprofils geöffnet hatte, was zu verlorenen Änderungen am Profil führte.
- Administratoren mussten RDP-Dateien mit fest kodierten Verbindungsnamen für diese einzelnen Anwendungen erstellen und verwalten. Wurde eine Anwendung aktualisiert, musste die RDP-Datei ebenfalls aktualisiert werden.

Kurz gesagt ist es verständlich, warum nicht wenige Benutzer einzelne Anwendungen von einem Vor-Windows Server 2008-Terminalserver angezeigt haben.

Windows Server 2008 führt RemoteApps für die Terminaldienste-Plattform zur Verwendung mit RDP 6.1 ein. RemoteApps zeigen einzelne Anwendungen an, doch ohne die vielen Nachteile eines Workarounds, eine RDP-Datei zu erstellen, die dafür vorgesehen ist, nur eine einzige Anwendung anzuzeigen:

- Die Anwendung besitzt die gleiche Titelleiste wie eine lokal ausgeführte Anwendung und wird in der Taskleiste nach ihrem Namen gekennzeichnet. Dadurch lässt sie sich leichter auffinden und sie passt auch besser zu lokalen Anwendungen.
- Alle vom selben Terminalserver gestarteten Anwendungen nutzen dieselbe Sitzung gemeinsam. Dadurch verringert sich die Belastung des Servers und alle Anwendungen können dieselbe Kopie des Benutzerprofils verwenden.
- RemoteApps können mit Terminaldienste-Webzugriff integriert werden, um Anwendungssymbole in einem Browser anzuzeigen und die Verbindungseinstellungen auf Anforderung festzulegen, sodass sie niemals veraltet sind.

Mehr über RemoteApps und wie sie mit Terminaldienste-Webzugriff verwendet werden, erfahren Sie in Kapitel 6.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

Rollen für Terminaldienste in Windows Server 2008

Gegenüber vorherigen Versionen unterscheiden sich die Rollen für Terminaldienste in Windows Server 2008 darin, dass die Rolle für wesentlich mehr als die beiden Aufgaben in vorherigen Versionen konzipiert ist. Bislang waren Terminaldienste die Antwort auf die Frage: »Wie kann ich diese Anwendungen auf einem gemeinsamen Server ausführen und wie kann ich den Zugriff auf diesen freigegebenen Server lizenzieren?« Jetzt ist das Spektrum wesentlich breiter. Terminaldienste beantworten Fragen wie zum Beispiel:

- Wie hoste ich Anwendungen, die viele Benutzer zur selben Zeit verwenden?
- Wie stelle ich diese Anwendungen in einem Webbrowser dar, um sicherzustellen, dass meine Endbenutzer über die neuesten Clientverbindungseinstellungen verfügen?
- Wie kann ich leicht Zugriff auf redundante freigegebene Server bereitstellen?
- Wie mache ich die freigegebenen Server für die Mitarbeiter zugänglich, die an Orten außerhalb des Büros arbeiten?
- Wie kann ich Remotezugriff auf die freigegebenen Server in meinem lokalen Netzwerk sichern?

Diese Fragen werden durch eine der fünf Rollendienste von Terminaldiensten in Windows Server 2008 beantwortet (siehe Abbildung 1.1).

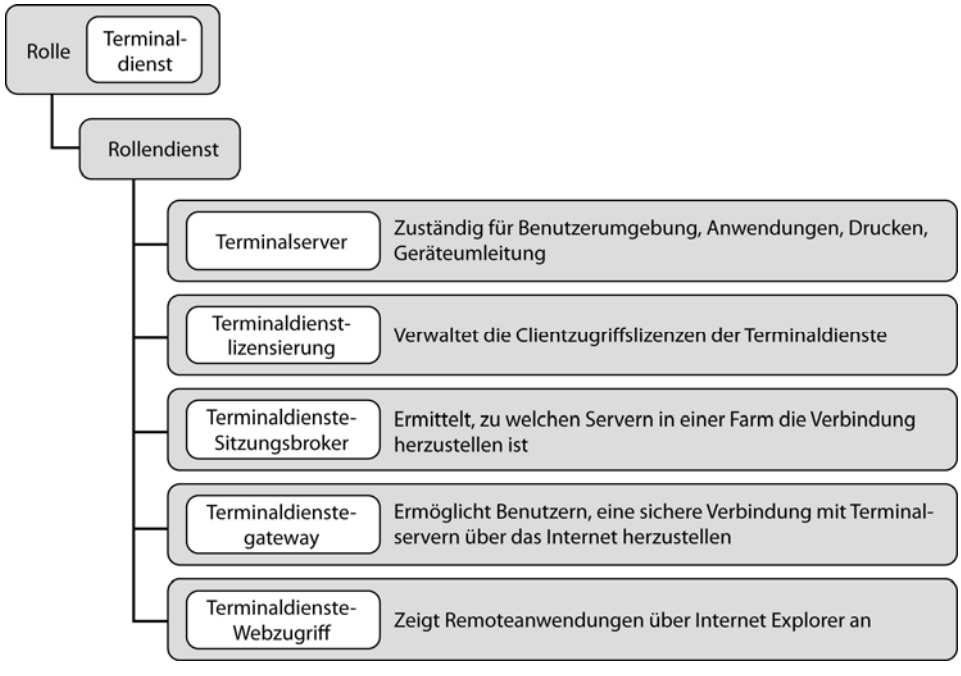

Abbildung 1.1 Die Rolle *Terminaldienste* umfasst fünf Rollendienste

Die folgenden Abschnitte gehen näher auf die fünf Rollendienste für Terminaldienste ein:

- Terminalserver
- Terminaldienstelizenzierung

- Terminaldienste-Sitzungsbroker
- Terminaldienstegateway
- Terminaldienste-Webzugriff

Terminalserver

Wie in früheren Versionen bleibt der Terminalserver der Kernbestandteil der Terminaldienste-Architektur. Letzten Endes laufen hier alle Anwendungen. Benutzer verbinden sich mit Terminalservern und starten Anwendungen, die auf den Servern installiert sind.

Ein Terminalserver unterscheidet sich in verschiedener Hinsicht von anderen Typen von Windows-Servern. Grundsätzlich funktioniert er mehr wie eine Workstation als ein Server. Zum Beispiel sind andere Serverrollen dafür konzipiert, einem allgemeinen Zweck zu dienen, beispielsweise E-Mails oder Datenbankabfragen zu bearbeiten. Ihre Prioritäten sind klar: Was immer im Vordergrund für den Zweck dieses Servers steht, erhält den Löwenanteil des Prozessors. Bei einem gemeinsam genutzten Server ist das anders. Da viele Personen ihn gleichzeitig verwenden, kann der Server nicht einfach annehmen, dass es sich bei der im Vordergrund laufenden Anwendung um diejenige handelt, die die gesamte Prozessorzeit erhalten sollte – welchen Vordergrund der vielleicht 40 Sitzungen sollte er herausgreifen? Demzufolge erhalten alle Benutzerprozesse auf einem Terminalserver die gleiche Priorität, sodass sie den Prozessor mehr oder weniger gleichmäßig unter allen Remotebenutzern auslasten.

Endbenutzer verbinden sich zu einem Terminalserver über eine RDP-Datei, die Verbindungsinformationen für den Server oder seine Farm speichert, oder über den Dienst Terminaldienste-Webzugriff, der Anwendungssymbole in einem Browser anzeigt, um schnell eine RDP-Datei zu erstellen. Wenn ein Benutzer eine Remotesitzung startet, ist sie gegenüber anderen Remotesitzungen, die auf diesem Computer laufen, geschützt. Endbenutzer können die Sitzungen untereinander nicht sehen. Zwar können sie sich versehentlich gegenseitig beeinflussen (indem zum Beispiel fordernde Anwendungen eingesetzt werden, die anderen Benutzern Prozessorzeit oder Speicher entziehen), doch gibt es kein Sicherheitsrisiko, wenn mehrere Benutzer auf demselben Terminalserver Sitzungen ausführen.

Terminalserver haben ein erhebliches Arbeitspensum zu bewältigen, um alle Remoteclientsitzungen zu unterstützen. Deshalb ist es im Allgemeinen am besten, Terminalserver ausschließlich für diesen Verwendungszweck zu reservieren.

Terminaldienste-Webzugriff

Terminaldienste-Webzugriff arbeitet mit IIS (Internet Information Services) zusammen, um ausgewählte Symbole der veröffentlichten Anwendungen in einem Portal anzuzeigen, das in Internet Explorer angezeigt wird. Ein Benutzer autorisiert sich gegenüber dem Portal und kann die Anwendungssymbole sehen. Klickt er auf ein Symbol, wird eine RemoteApp-Anwendung in fast der gleichen Weise erstellt und gestartet, als wenn die RDP-Datei auf dem Computer des Endbenutzers gespeichert wäre.

Terminaldienste-Webzugriff ist ein Rollendienst für die Rolle *Terminaldienste*, der es ermöglicht, RemoteApp-Programme zu erstellen. Zudem ist er auch eine Verknüpfung zum Terminalserverdesktop, der Benutzern vom Internet Explorer aus zugänglich ist. Darüber hinaus versetzt Terminaldienste-Webzugriff Benutzer in die Lage, sich von einem Webbrowser mit dem Remotedesktop eines beliebigen Server- oder Clientcomputers zu verbinden, auf die sie den geeigneten Zugriff besitzen.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

Ein Benutzer kann mit Terminaldienste-Webzugriff eine Website besuchen (entweder vom Internet oder von einem Intranet aus), um auf eine Liste der verfügbaren RemoteApp-Programme zuzugreifen. Wenn ein Benutzer ein RemoteApp-Programm startet, wird eine Terminaldienstesitzung auf dem Windows Server 2008-basierten Terminalserver gestartet, der das RemoteApp-Programm hostet. Der Terminaldienste-Webzugriff-Server startet die Anwendung nicht. Wie aus Abbildung 1.2 hervorgeht, zeigt er lediglich das Anwendungssymbol an, erstellt die RDP-Datei für die Anwendung, wenn der Endbenutzer auf das Symbol doppelklickt (1), und übergibt dann die RDP-Datei an den Endbenutzer, um die Anwendung vom Terminalserver aus zu starten (2). Die via Terminaldienste-Webzugriff gestarteten RemoteApps und Desktops werden nicht im Browser angezeigt, sondern in ihren eigenen Fenstern (3), und sind unabhängig vom Browserfenster.

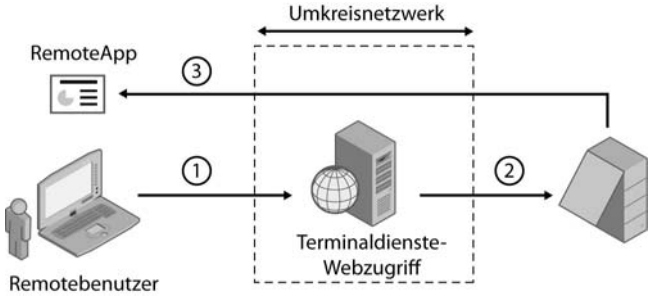

Abbildung 1.2 Terminaldienste-Webzugriff zeigt Anwendungssymbole in einem Browser als Komfort für Endbenutzer an

Terminaldienste-Webzugriff besitzt unter anderem folgende Vorteile:

- Benutzer können auf RemoteApp-Programme von einer Website über das Internet oder von einem Intranet aus zugreifen. Um ein RemoteApp-Programm zu starten, muss der Benutzer lediglich auf das Programmsymbol doppelklicken.
- Wenn ein Benutzer mehr als ein RemoteApp-Programm über Terminaldienste-Webzugriff startet und die Programme auf demselben Terminalserver ausgeführt werden, laufen die RemoteApp-Programme innerhalb derselben Terminaldienstesitzung. Dadurch bleibt nur eine einzige Kopie des Benutzerprofils geöffnet und der Overhead auf dem Terminalserver verringert sich.
- Durch den Einsatz von Terminaldienste-Webzugriff entsteht wesentlich weniger administrativer Overhead, als erforderlich ist, um RDP-Dateien für die Verbindung zu einer Terminalserverfarm zu verwalten und zu verteilen. Programme lassen sich leicht von einem zentralen Ort aus bereitstellen und Sie müssen sich keine Gedanken darum zu machen, dass RDP-Dateien mit Verbindungsdaten immer auf dem neuesten Stand sind. Und da die Programme auf einem Terminalserver und nicht auf dem Clientcomputer laufen, sind sie leichter zu warten.
- Terminaldienste-Webzugriff umfasst Remotedesktop-Webverbindung, was Benutzer in die Lage versetzt, sich remote mit dem Desktop jedes beliebigen Computers zu verbinden, wo sie Remotedesktopzugriff vom Portal der Terminaldienste-Webzugriff haben.
- Terminaldienste-Webzugriff arbeitet mit einer minimalen Konfiguration, doch umfasst die Terminaldienste-Webzugriffsseite ein anpassbares Webpart, das sich in eine benutzerdefinierte Webseite oder eine Microsoft SharePoint-Website einbinden lässt.

Kapitel 6 geht ausführlicher darauf ein, wie Sie Terminaldienste-Webzugriff konfigurieren und verwenden – und welche Einschränkungen zu beachten sind.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

Terminaldienste-Sitzungsbroker

Aus Redundanzgründen empfiehlt es sich, den Satz der Remoteanwendungen auf mehreren Terminalservern zu hosten und einen Lastenausgleich für die Server einzurichten. Damit lässt sich die Arbeitslast verteilen, die durch die Benutzer entsteht, und es sinkt die Wahrscheinlichkeit, dass Ihnen ein ausgefallener Server die Möglichkeit nimmt, zentralisierte Anwendungen zu bedienen. Problematisch dabei ist, dass Verbindungen grundsätzlich zu einzelnen Terminalservern und nicht zu Servergruppen hergestellt werden – d.h. dass letzten Endes die endgültige Verbindung zum Terminalserver mit dem Namen *TS1* (oder einem anderen originellen Namen, den Sie ihm gegeben haben) eingerichtet wird. Doch wenn Ihre RDP-Dateien die Namen individueller Terminalserver enthalten, nehmen sie nicht am Lastenausgleich teil. Zudem sind sie auch nicht flexibel genug, um zu ermitteln, dass ein Benutzer eigentlich mit einem anderen Terminalserver verbunden werden sollte, wenn er eine neue Anwendung startet, da er dort bereits eine Anwendung geöffnet hat.

Terminaldienste-Sitzungsbroker ist dafür zuständig zu ermitteln, zu welchem Terminalserver eine eingehende Verbindung gehen sollte, wenn sich der Benutzer mit einer Farm verbindet, wie es in Abbildung 1.3 zu sehen ist. Terminaldienste-Sitzungsbroker trifft diese Entscheidung anhand mehrerer Kriterien. Unter anderem wird ausgewertet,

- zu welcher Farm die eingehende Anforderung die Verbindung herzustellen versucht,
- ob die Person, von der die Verbindungsanforderung stammt, bereits über eine vorhandene (aktive oder getrennte) Sitzung auf dieser Farm verfügt,
- welcher Terminalserver die kleinste Anzahl von Sitzungen hat.

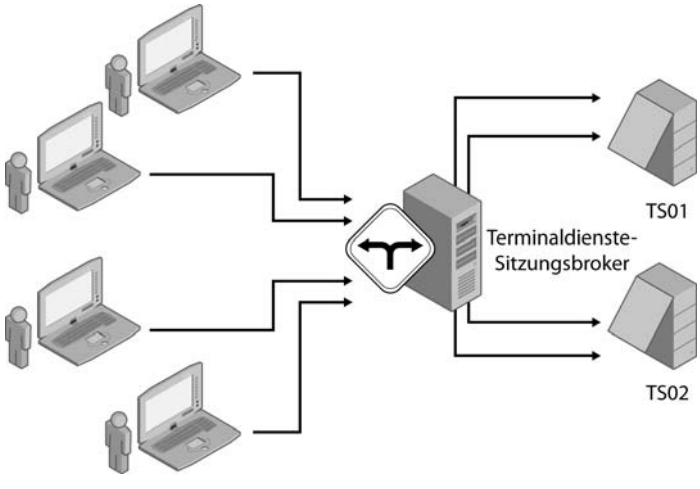

Abbildung 1.3 Der Terminaldienste-Sitzungsbroker leitet eingehende Verbindungen an den geeigneten Server weiter

Der Terminaldienste-Sitzungsbroker beherrscht nur eine Form des Lastenausgleichs – er überwacht, wie viele Sitzungen Terminalserver haben. Es ist aber möglich, Lastenausgleichsmodule von Drittanbietern zu integrieren, die andere Kriterien wie zum Beispiel Prozessor-/Speicherbelastung, Uhrzeit oder Anwendung unterstützen. Mehr zu Terminaldienste-Sitzungsbroker erfahren Sie in Kapitel 7.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

Terminaldienstegateway

In den dunklen Zeiten vor Windows Server 2008 mussten Sie Port 3389 öffnen (den Port, auf den RDP hört), wenn Sie sich ausschließlich mit Bordmitteln von einem externen Standort mit einem Terminalserver verbinden wollten, damit der Terminalserver eingehende Verbindungen akzeptieren konnte. Die meisten Benutzer haben aufgrund des Sicherheitslochs, das über den zusätzlichen Port aufgetan wurde, darauf verzichtet.

Zu den Rollendiensten von Terminaldiensten in Windows Server 2008 gehört Terminaldienstegateway. Dieser Dienst ermöglicht autorisierten Benutzern, die Verbindung zu Ressourcen in einem internen Firmennetz oder privaten Netzwerk von jedem Gerät mit Internetanschluss aus herzustellen, egal ob es ursprünglich Teil der Domäne oder ein öffentlicher Kiosk war. Wie Abbildung 1.4 zeigt, kann es sich bei Netzwerkressourcen um Terminalserver, die vollständige Desktops unterstützen, Terminalserver, die RemoteApp-Programme ausführen, oder Computer mit aktiviertem Remotedesktop handeln. Mit anderen Worten können Benutzer, die auf das Firmennetzwerk vom Internet aus zugreifen, vollständige Desktops, einzelne Anwendungen oder sogar ihre eigenen Desktopcomputer verwenden – das hängt alles davon ab, was der Administrator eingerichtet hat.

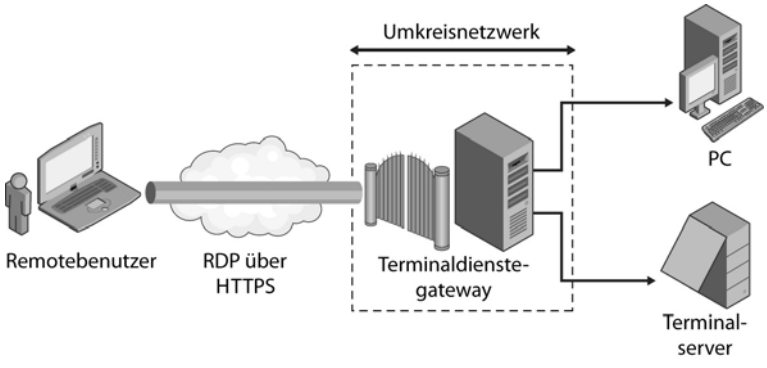

Abbildung 1.4 Terminaldienstegateway realisiert sicheren Zugriff auf das Firmennetzwerk vom Internet aus

Terminaldienstegateway richtet mithilfe von RDP über HTTPS eine sichere verschlüsselte Verbindung zwischen Remotebenutzern im Internet und dem internen Netzwerk ein, in dem ihre Anwendungen laufen. Dazu muss lediglich Port 443 geöffnet werden (der bereits für sichere Internetverbindungen geöffnet ist). Somit kann Terminaldienstegateway

- Remotebenutzern ermöglichen, eine verschlüsselte Verbindung über das Internet zu internen Netzwerkressourcen herzustellen, ohne VPN (Virtual Private Network)-Verbindungen konfigurieren zu müssen.
- ein umfangreiches Sicherheitskonfigurationsmodell bereitstellen, mit dem Sie den Zugriff auf spezifische interne Netzwerkressourcen steuern können.
- eine Punkt-zu-Punkt-RDP-Verbindung bereitstellen, die sich einschränken lässt, anstatt Remotebenutzern den Zugriff auf sämtliche internen Netzwerkressourcen zu gestatten.
- die meisten Remotebenutzer in die Lage versetzen, sich mit internen Netzwerkressourcen hinter Firewalls in privaten Netzwerken und über Netzwerkadressübersetzung (Network Address Translation, NAT) zu verbinden. In diesem Szenario brauchen Sie mit Terminaldienstegateway keine zusätzliche Konfiguration für den Terminaldienste-Gatewayserver oder die Clients durchzuführen.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

Die Snap-In-Konsole *Terminaldienstegateway-Manager* ermöglicht Ihnen, Autorisierungsrichtlinien zu konfigurieren, um Bedingungen zu definieren, die für Remotebenutzer erfüllt sein müssen, damit sie sich mit internen Netzwerkressourcen verbinden können. Zum Beispiel können Sie festlegen,

- wer sich mit Netzwerkressourcen verbinden darf (d.h. die Benutzer- oder Computergruppen, die die Verbindung herstellen können).
- mit welchen Netzwerkressourcen (Computergruppen) sich Benutzer verbinden können.
- ob Geräte- und Datenträgerumleitung zulässig ist.
- ob Clients Smartcardauthentifizierung oder Kennwortauthentifizierung verwenden müssen oder beide Methoden verwenden können.

Terminaldienste-Gatewayserver und Terminaldienstеclients lassen sich für Netzwerkzugriffsschutz (Network Access Protection, NAP) konfigurieren, um die Sicherheit weiter zu erhöhen. NAP ist eine Technologie zur Erstellung von Clientintegritätsrichtlinien, Integritätserzwingung und Integritätswiederherstellung, die in Windows XP SP3, Windows Vista und Windows Server 2008 eingebunden ist. Mithilfe von NAP können Systemadministratoren Integritätsanforderungen erzwingen – u.a. für Softwareanforderungen, Anforderungen an Sicherheitsaktualisierungen oder erforderliche Computerkonfigurationen.

HINWEIS Wenn Terminaldienstegateway NAP erzwingt, lassen sich Computer, die unter Windows Server 2008 laufen, nicht als NAP-Clients einsetzen. In diesem Fall kommen nur Computer als NAP-Clients infrage, die unter Windows XP SP3 oder Windows Vista laufen.

Sie können auch Terminaldienste-Gatewayserver mit Microsoft ISA (Internet Security and Acceleration)-Server einsetzen, um die Sicherheit zu erweitern. In diesem Szenario können Sie Terminaldienste-Gatewayserver in einem privaten Netzwerk statt im Umkreisnetzwerk und ISA-Server im Umkreisnetzwerk hosten. Die SSL-Verbindung zwischen dem Terminaldienstеclient und dem ISA-Server kann am ISA-Server mit Internetzugang terminiert werden.

Die Snap-In-Konsole *Terminaldienstegateway-Manager* stellt Tools bereit, mit denen Sie Status, Integrität und Ereignisse von Terminaldienstegateway überwachen können. Mit dem Terminaldienstegateway-Manager können Sie Ereignisse (wie zum Beispiel nicht erfolgreiche Verbindungsversuche zum Terminaldienste-Gatewayserver) spezifizieren, die Sie überwachen möchten.

Es ist möglich, Terminaldienstegateway lediglich mit einer Terminalserverfarm und RDP-Dateien, die auf Clientcomputern gespeichert sind, oder mit Terminaldienste-Webzugriff zu verwenden. In Verbindung mit Terminaldienste-Webzugriff können Sie einen Remotearbeitsbereich einrichten, der eine Website mit den Anwendungssymbolen präsentiert, und dann sicherstellen, dass die Benutzer, die die Verbindung herstellen, oder der Computer, von dem aus die Benutzer die Verbindung herstellen, den Terminaldienstegateway-Regeln entsprechen.

Terminaldienstegateway kommt mit wenigen Ressourcen aus und kann Hunderte eingehende Benutzer unterstützen, sodass sich dieser Dienst problemlos mit anderen Rollen im Umkreisnetzwerk kombinieren lässt.

Terminaldienstelizenzierung

Der Rollendienst *Terminaldienstelizenzierung* überwacht, wer eine Lizenz besitzt, den Terminalserver zu verwenden. Es geht nicht darum, wer autorisiert ist, den Terminalserver zu verwenden – das erledigen Active Directory-Benutzerrechte und/oder Terminaldienstegateway, abhängig davon, auf welcher Stufe der

Administrator diese Verbindung autorisiert. Terminaldienstelizenzierung ist das Lizenzverwaltungssystem, das Terminalserver in die Lage versetzt, Terminaldienste-Clientzugriffslizenzen für Geräte und Benutzer, die sich mit einem Terminalserver verbinden, abzurufen und zu verwalten.

HINWEIS Terminaldienstelizenzierung unterstützt Terminalserver, die unter Windows Server 2008 laufen, sowie Terminalserver, die unter Windows Server 2003 oder Windows Server 2000 laufen. Das Betriebssystem unterstützt zwei parallele Verbindungen, um einen Computer remote zu verwalten, sodass Sie für diese Verbindungen keinen Lizenzserver brauchen.

Auf die Terminaldienstelizenzierung geht zwar Kapitel 3 detailliert ein, doch sollten Sie zumindest das Prinzip kennen: Der Terminalserver ermittelt, ob der Benutzer oder der Computer, der die Verbindung zum Server herstellt, über eine gültige Lizenz verfügt. Ist das der Fall, lässt der Terminalserver die Verbindung zu. Andernfalls versucht der Terminalserver, einen Lizenzserver zu kontaktieren, um festzustellen, ob eine Lizenz für dieses Gerät oder diesen Benutzer verfügbar ist. Der Lizenzserver weist dann entweder dem Gerät eine Lizenz zu oder bearbeitet die Eigenschaften des Benutzerkontos in Active Directory, um zu zeigen, dass eine Lizenz verwendet worden ist. Kann der Terminalserver keine Verbindung zu einem Terminaldienste-Lizenzierungsserver herstellen, stellt er eine temporäre Lizenz aus, wenn der Terminalserver innerhalb seines Aktivierungszeitraums läuft. Diese temporäre Lizenz ist nur für 120 Tage gültig.

Server, die die Rolle Terminaldienstelizenzierung unterstützen, verwalten eine Datenbank, die überwacht, wie Terminaldienste-Clientzugriffslizenzen ausgestellt wurden. Bei Terminaldienste-Clientzugriffslizenzen pro Gerät wird die Lizenz einem Computer zugewiesen. Dagegen wird eine Lizenz des Typs pro Benutzer nicht wirklich zugewiesen – es wird nur ihre Verwendung verfolgt.

Terminaldienstelizenzierung ist ein »anspruchsloser« Dienst, der für normale Operationen kaum CPU oder Speicher belastet. Der Speicherbedarf bleibt unterhalb von 10 MB. Die Festplattenanforderungen sind gering, selbst für eine erhebliche Anzahl von Clients. Die Lizenzdatenbank wächst in Inkrementen von 5 MB für jeweils 6.000 ausgestellte TS-Clientzugriffslizenzen. Der Lizenzserver ist nur aktiv, wenn ein Terminalserver eine TS-Clientzugriffslizenz anfordert, und sein Einfluss auf die Serverleistung ist selbst in Szenarios mit hoher Belastung kaum zu spüren. Demzufolge kann in kleineren Bereitstellungen die Rolle TS-Lizenzierung auf demselben Computer wie der Rollendienst Terminalserver installiert werden. In größeren Bereitstellungen wird die Rolle TS-Lizenzierung oftmals auf einem separaten Computer realisiert.

Mehr zur Terminaldienstelizenzierung erfahren Sie in Kapitel 3.

Die Umgebung der Windows Server 2008-Terminaldienste verstehen

Die Rolle *Terminaldienste* existiert nicht in einem Vakuum. Mehrere Rollen helfen dabei, die verschiedenen Rollendienste von Terminaldiensten zu unterstützen, und ohne sie funktioniert die Lösung nicht. Außer den Kernrollendiensten von Terminaldiensten und ihren Beziehungen untereinander ist es wichtig, ihre Beziehungen zu anderen Windows Server-Rollen zu verstehen. Dieser Abschnitt erläutert, was diese Rollen sind und wie sie die Funktionalität von Terminaldiensten unterstützen.

Was sind das für Rollen und wie passen sie zu zusammen? Wie passen sie zu den anderen Bestandteilen der Windows-Infrastruktur, die nicht zu Terminaldiensten gehören (IIS, Zertifikate, Active Directory usw.)? Dies ist eine Beschreibung der Systemarchitektur, kein Bereitstellungshandbuch.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

Die Clientverbindung

Auch wenn es auf der Hand liegt, lohnt ein Blick darauf: Das Benutzerszenario wird durch die Art und Weise definiert, wie der Client mit den Rollendiensten von Terminaldiensten interagiert.

Die grundlegende Beziehung zwischen Client und Server besteht aus drei Teilen: dem RDC-Client, der RDP-Verbindung und dem Server.

HINWEIS Weshalb unterscheidet man zwischen RDP und RDC? Das Remotedesktopprotokoll (Remote Desktop Protocol, RDP) ist das Protokoll, das Benutzereingaben und Anwendungsausgaben zwischen Client und Server übergibt. Die Remotedesktopverbindung (Remote Desktop Connection, RDC) ist die Clientkomponente, die die RDP-Verbindung initiiert und verwaltet.

- Die RDC-Clientkomponente initiiert die Verbindung zum Server und empfängt die Daten, die der Server an sie sendet.
- Die Serverkomponente interagiert mit dem Kernbetriebssystem und übernimmt die empfangenen Informationen (d.h. Daten für die Sounderzeugung oder anzuzeigende Bitmaps), konvertiert sie in RDP-Befehle und serialisiert sie, um sie an den Client zu übergeben.
- Das Protokoll aktiviert die Verbindung zwischen dem Client und dem Server; es definiert die Art der Informationen, die zwischen ihnen über virtuelle Kanäle übertragen werden.

Kurz gesagt fordert der Client die Verbindung an, der Server formatiert die Aufrufe zu den Anwendungen und zum Betriebssystem in einer Weise, die der Client verstehen kann (oder der Server, je nachdem, auf welchem Weg der Informationsfluss für eine bestimmte Transaktion arbeitet), und RDP-Durchläufe lassen den Benutzer mit den Anwendungen auf dem Server so kommunizieren, als würden sie lokal ausgeführt.

Virtuelle Kanäle sind bidirektionale Verbindungsstreams, die über RDP bereitgestellt werden. Sie richten eine Datenpipe zwischen dem RDC-Client und dem Terminalserver ein, um bestimmte Arten von Informationen – beispielsweise Geräteumleitung oder Sounddaten – zwischen Client und Server zu übergeben. Windows 2000 hat mit virtuellen Kanälen die Funktionalität von RDP erweitert und auch einige Terminaldienste-Features wie zum Beispiel Geräte- und Soundumleitung greifen auf virtuelle Kanäle zurück.

Doch seit Windows 2000 Server hat sich eine Menge geändert. Unter anderem gilt das für die 32 virtuellen Kanäle, die ursprünglich in RDP 5.1 verfügbar waren und die nun nicht mehr ausreichen. Es gibt jetzt mehr Datenarten und es liegt es auf der Hand, dass noch weitere hinzukommen können, die noch nicht berücksichtigt wurden. Außerdem wiesen virtuelle Kanäle ein Problem auf: Sie wurden am Beginn der Verbindung erstellt und am Ende abgebaut. Wenn Sie ein Gerät hinzugefügt haben, während der RDP-Client verwendet wurde, konnte es virtuelle Kanäle erst dann verwenden, wenn die Verbindung beendet und dann erneut hergestellt wurde.

HINWEIS Beim Beenden einer Sitzung wird diese auf dem Server endgültig beendet. Zu einer getrennten Sitzung lässt sich wieder eine Verbindung herstellen.

Demzufolge unterstützen Terminaldienste in Windows Server 2008 *dynamische Kanäle* – virtuelle Kanäle, die der Client auf Anforderung erzeugt und wieder schließt, wenn er sie nicht mehr benötigt. Wenn Sie wissen möchten, wie die Schnittstellen aussehen, damit Sie dynamische Kanäle nutzen können (oder wie sie überhaupt funktionieren), lesen Sie den Abschnitt »Neue Funktionalität für Partner von Terminaldiensten« später in diesem Kapitel.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

Server- und Clientcomputer mit Zertifikaten authentifizieren

Zu den seltsamen Dingen bei Terminaldiensten gehört das erforderliche Vertrauen zwischen Client und Server. Offensichtlich muss der Server dem Client vertrauen, da der Server gewissermaßen eine Tür zum Firmennetzwerk darstellt. Doch der Client muss dem Server ebenfalls vertrauen. Da der Client den Benutzernamen und das Kennwort für das Firmennetz bereitstellt, muss der Server, mit dem sich der Client verbindet, ein legitimer Terminalserver und kein so genannter Rogue-Server sein, der Anmeldeinformationen beschaffen soll.

Um sich zu vergewissern, dass Client und Server diejenigen sind, die sie vorgeben zu sein, können Sie je ein Zertifikat auf dem Server und auf dem Client installieren. Dazu brauchen Sie einen Zertifikatserver, um die Zertifikate zu verwalten, oder Sie kaufen Zertifikate von einer öffentlichen Zertifizierungsstelle.

HINWEIS Alle Terminalserver in derselben Farm verwenden dasselbe Zertifikat. Das ist heute der einzige Weg, damit Sie sich selbst nach der gleichen Methode gegenüber dem Client authentifizieren können.

RemoteApp-Programme für Terminaldienste-Webzugriff anzeigen

Terminaldienste besitzen keine Webkomponente für die Anzeige von Anwendungen in einem Portal. Damit Terminaldienste-Webzugriff funktioniert, müssen Sie einen IIS-Server einrichten, um die Site zu hosten, die das Portal anzeigt.

Benutzer- und Computereinstellungen aktualisieren

Active Directory ist eine derartig offensichtliche Wahl für eine Unterstützungsrolle, dass man es fast übersieht. Es ist jedoch entscheidend für eine funktionierende zentralisierte Infrastruktur – und zwar auf mehrere Arten, die Sie vielleicht gar nicht alle erwartet haben. Active Directory ist unter anderem dafür zuständig,

- die Gruppenrichtlinien zu verwalten, mit denen Terminalserver und die auf ihnen laufenden Benutzersitzungen konfiguriert werden.
- festzustellen, ob ein Benutzer über die Berechtigung verfügt, sich mit einem Terminalserver zu verbinden.
- die Anzeige zu realisieren, dass ein Benutzer eine Terminaldienste-Clientzugriffslizenz (pro Benutzer) verbraucht hat.

Neue Funktionalität für Partner von Terminaldiensten

Terminaldienste sind nicht einfach ein Produkt – selbst wenn das prinzipiell zutrifft –, sondern auch eine Entwicklungsplattform, mit der sowohl ISVs als auch Berater benutzerdefinierte Lösungen erstellen können. Unter diesem Aspekt erläutert dieser Abschnitt die Funktionalität, die Terminaldienste von Windows Server 2008 in Form öffentlicher Schnittstellen für die Anpassung bieten.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

HINWEIS Öffentliche Schnittstellen (so genannte Application Programming Interfaces, APIs) sind Schnittstellen, die – wie schon ihr Name sagt – öffentlich verfügbar sind und in MSDN dokumentiert werden, sodass Berater und unabhängige Softwareanbieter (ISVs) darauf zurückgreifen können. Private Schnittstellen werden nicht dokumentiert. Der wesentliche Unterschied zwischen ihnen besteht in den Unterstützungsmöglichkeiten. Eine private Schnittstelle kann der Entwickler (in diesem Fall Microsoft) jederzeit ändern, wenn es sich erforderlich macht. Eine API wird nicht ohne Vorankündigung geändert. Wenn Sie dagegen mit privaten Schnittstellen programmieren, wissen Sie nie, wann das Tool, an dem Sie so hart gearbeitet haben, infolge einer Codeänderung im Betriebssystem versagt. Selbst wenn Sie die Möglichkeit hätten, Projekte auf privaten Schnittstellen basierend zu erstellen, wäre es besser, sich ausschließlich auf die öffentlichen APIs statt auf die privaten zu stützen.

APIs von Terminaldiensten

Genau genommen sind APIs für Terminaldienste nicht neu. Die erste Gruppe öffentlicher Schnittstellen, die Microsoft verfügbar gemacht hat, waren die WTS (Windows Terminal Server)-Schnittstellen, die mit Service Pack 4 für Windows NT 4.0 Terminal Server Edition eingeführt und in Windows 2000 Server öffentlich gemacht wurden. Lange Zeit waren sie die Basis für die Befehlszeilentools der Terminaldienste wie zum Beispiel *Qwinsta.exe* und *Query.exe*. Es gibt vier Gruppen von WTS-APIs:

- **Sitzungsverwaltung** Wird verwendet, um Sitzungen und Prozesse auf einem Terminalserver aufzulisten und zu verwalten. Außerdem können Sie damit die Verbindung zu anderen Terminalservern in der Domäne herstellen.
- **Client/Server-Kommunikation** Verwenden Sie virtuelle Kanäle von Terminaldiensten, um zwischen Client- und Serverkomponenten einer Anwendung auf zwei verschiedenen Computern zu kommunizieren.
- **Virtuelle Kanäle** Wird verwendet für die Erweiterung von Client/Server-Anwendungen in einer Terminaldiensteumgebung.
- **Benutzerkonfiguration** Wird verwendet, um Terminaldienste-spezifische Konfigurationsinformationen festzulegen und abzurufen.

APIs für die Sitzungsverwaltung

Die APIs für die Sitzungsverwaltung haben sich praktisch nicht geändert, seit die WTS-APIs erstmals veröffentlicht wurden. Tabelle 1.1 beschreibt diese API-Funktionen. Wenn Sie schon länger mit Terminaldiensten arbeiten, dürfte Ihnen die Funktionalität von den Befehlszeilentools und der Terminaldienstesverwaltung her bekannt vorkommen.

API	Beschreibung	Verwendet von
WTSDisconnectSession	Trennt den Client von einer bestimmten Sitzung. Die Sitzung bleibt aktiv und der Benutzer kann sich wieder anmelden, um sich mit derselben Sitzung zu verbinden.	*Tsdiscon* *Trennen*-Operation der Terminaldienste-verwaltung
WTSEnumerateSessions	Gibt eine Liste der Sitzungen auf dem angegebenen Terminalserver zurück.	*Query session* Registerkarte *Sitzungen* der Terminaldienste-verwaltung ▶

API	Beschreibung	Verwendet von
WTSEnumerateProcesses	Gibt eine Liste der Prozesse auf dem angegebenen Terminalserver zurück.	*Query process* Registerkarte *Prozesse* der Terminaldienste-verwaltung
WTSLogoffSession	Meldet die angegebene Sitzung ab.	
WTSQuerySessionInformation	Gibt Informationen über die angegebene Sitzung auf dem angegebenen Terminal-server zurück.	*Query session* Registerkarte *Sitzungen* der Terminaldienste-verwaltung
WTSSendMessage	Zeigt ein Meldungsfeld auf der Clientanzeige der angegebenen Sitzung(en) an.	*Msg* Funktion *Nachricht senden* der Terminal-diensteverwaltung
WTSShutdownSystem	Fährt einen Terminalserver herunter und startet ihn optional neu.	Dieser nicht mehr verfügbare Befehl wurde verwendet, um mit *tsshutdn* verbunden zu werden.
WTSTerminateProcess	Beendet den angegebenen Prozess auf dem angegebenen Terminalserver.	*Tskill* Registerkarte *Prozesse* der Terminaldienste-verwaltung
WTSVirtualChannelOpen	Öffnet einen Handler zur Serverseite des angegebenen virtuellen Kanals. Weitere Informationen zu virtuellen Kanälen finden Sie im Abschnitt »Die Clientverbindung« weiter vorn in diesem Kapitel.	
WTSWaitSystemEvent	Wartet auf ein Ereignis, beispielsweise das Erstellen einer Clientsitzung oder eine Benutzeranmeldung am Terminalserver.	

Tabelle 1.1 WTS-APIs in Windows Server 2008

APIs für Client/Server-Kommunikation

Unter dem Blickwinkel der Terminaldienste besteht der Client/Server-Hauptbedarf an Schnittstellen darin, sicherzustellen, dass die Kommunikation zwischen der korrekten Instanz des Clients, der auf dem Terminal-server läuft, und dem Back-End-Server eingerichtet wird. Die Serverkomponente kann auch auf öffentliche Schnittstellen zurückgreifen, um Nachrichten an den Client zu senden. Tabelle 1.2 gibt die Funktion und die Schnittstellen an, die diese Fähigkeiten ermöglichen.

API/Funktion	Beschreibung	Verwendet für
ProcessIdToSessionId	Ordnet die PID der Clientkomponente einer bestimmten Sitzung zu.	Von der Clientkomponente einer Client-Server-Anwendung verwendet, um die Sitzungs-ID abzurufen, sodass sie diese Informationen an die Serverkomponente übergeben kann. Die Serverkomponente kann dann diese Informationen verwenden, um einen privaten Kommunikationskanal einzurichten. ▶

API/Funktion	Beschreibung	Verwendet für
WTSQuerySessionInformation	Gibt Informationen über die angegebene Sitzung auf dem angegebenen Terminalserver zurück.	In diesem Fall von der Serverkomponente verwendet, um zusätzliche Informationen über den Client abzurufen.
WTSSendMessage	Zeigt ein Meldungsfeld auf der Clientanzeige der angegebenen Sitzung(en) an.	Kann in diesem Fall von der Serverkomponente verwendet werden, um eine Nachricht an die Clientkomponente zu senden.

Tabelle 1.2 Client/Server-Kommunikation in einer Terminaldiensteumgebung aktivieren

APIs für virtuelle Kanäle

Die in Tabelle 1.3 aufgeführten APIs für virtuelle Kanäle werden in erster Linie von Entwicklern verwendet und nicht von Terminalserver-Beratern, die Skriptlösungen erstellen. Die hier aufgeführten Funktionen sind für statische Kanäle vorgesehen, die zu Beginn einer Sitzung erstellt und am Ende der Sitzung wieder verworfen werden. Terminaldienste in Windows Server 2008 unterstützen auch dynamische virtuelle Kanäle, die im Verlauf der Sitzung erstellt und zerstört werden können, um auf Änderungen der Umgebung zu reagieren (wenn zum Beispiel ein clientseitiges Gerät angesteckt wird). Die Schnittstelle *IWTSPlugin* unterstützt dynamische virtuelle Kanäle, indem sie die virtuellen Kanäle einrichtet und abbaut.

API	Beschreibung
WTSVirtualChannelClose	Schließt einen offenen Handle für einen virtuellen Kanal.
WTSVirtualChannelPurgeInput	Löscht alle in die Warteschlange gestellten Eingabedaten, die der Client an den Server in einem bestimmten virtuellen Kanal gesendet hat.
WTSVirtualChannelPurgeOutput	Löscht alle in die Warteschlange gestellten Ausgabedaten, die der Server an den Client in einem bestimmten virtuellen Kanal gesendet hat.
WTSVirtualChannelQuery	Gibt Informationen über einen bestimmten virtuellen Kanal zurück.
WTSVirtualChannelRead	Liest Daten von der Serverseite eines virtuellen Kanals.
WTSVirtualChannelWrite	Schreibt Daten an die Serverseite eines virtuellen Kanals.
VirtualChannelInit	Registriert die Namen der virtuellen Kanäle, die vom Client verwendet werden, und stellt eine *VirtualChannelInitEvent*-Callback-Funktion bereit, über die Terminaldienste den Client über Ereignisse benachrichtigen, die die Clientverbindung beeinflussen.
VirtualChannelOpen	Öffnet die Clientseite eines bestimmten virtuellen Kanals und stellt einen Pfad bereit, über den Terminaldienste den Client über Ereignisse benachrichtigen, die den virtuellen Kanal beeinflussen.
VirtualChannelWrite	Schreibt Daten in einen virtuellen Kanal. Terminaldienste senden diese Daten an die Serverseite des virtuellen Kanals, wo der Server die Daten liest.
VirtualChannelClose	Schließt einen virtuellen Kanal.

Tabelle 1.3 APIs für virtuelle Kanäle

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

APIs für Benutzerkonfiguration

Die Enumeration *WTS_CONFIG_CLASS* konfiguriert Sitzungseigenschaften für viele Sitzungseinstellungen (z.B. Laufwerkumleitung, ob der Standarddrucker des Clients zum Standarddrucker für die Sitzung wird und Einstellungen, die das Verhalten festlegen, wenn die Sitzung getrennt wird) und richtet sie auf Benutzerbasis statt auf Pro-Server-Basis ein. Diese Eigenschaften legen Sie mit *IADsTSUserEx* fest.

Windows-Verwaltungsinstrumentation

Eigentlich ist dies nicht der richtige Platz, um die Grundlagen der Windows-Verwaltungsinstrumentation (Windows Management Instrumentation, WMI) zu behandeln, doch einige Hintergrundinformationen dürften hilfreich sein. Als Einsteiger in WMI sollten Sie sich näher mit diesem Thema befassen, bevor Sie diese Schnittstellen für die Verwaltung der Terminaldienste verwenden. Die Seite »Windows Management Instrumentation« auf der MSDN-Website von Microsoft (derzeit unter *http://msdn2.microsoft.com/en-us/library/aa394582(VS.85).aspx*) bildet einen guten Ausgangspunkt dafür.

WMI stellt im Wesentlichen einen Weg dar, einen Computer zu beschreiben, und zwar sowohl in Bezug auf Hardware (wie Netzwerkadapter, Festplatten) als auch auf Software (einschließlich der Dienste). Von höherer Warte aus können Sie die Elemente in einem Computer in Form von Klassen wie zum Beispiel *Festplatten* oder *Terminaldienste-Gatewayserver* beschreiben. Auf systemnaher Ebene können Sie spezifischer auf die einzelnen Instanzen dieser Festplatten oder eine Verbindung zu einem dieser Terminaldienste-Gatewayserver eingehen.

Genau genommen ist die Unterstützung für WMI ebenfalls nicht neu in Windows Server 2008. Doch obwohl Terminaldienste in Windows Server 2003 einige WMI-Objekte für die Verwaltung der Terminaldienste-Umgebung eingebunden hat, bringt Windows Server 2008 wesentlich mehr und teilweise vollkommen neue Klassen für Terminaldienstelizenzierung, Terminaldienstegateway und RemoteApps mit. Die folgenden Abschnitte und Tabellen sollen Ihnen in Form einer Schnellreferenz zeigen, wofür die Klassen konzipiert sind und was in Windows Server 2008 neu ist. In der MSDN-Dokumentation finden Sie ausführliche Details, wie Sie diese Klassen verwenden können. Momentan genügt es, wenn Sie sich die Tabellen ansehen, um einen Eindruck davon zu bekommen, was Sie mit diesen Schnittstellen tun können. Wenn es zweckmäßig ist, zeigen wir an den entsprechenden Stellen im Buch, wie Sie diese Klassen in Skripts einsetzen.

HINWEIS Obwohl WMI in der Vergangenheit über Skriptsprachen wie zum Beispiel VBScript verwendet wurde, ist es unserer Ansicht nach über Windows-PowerShell zugänglicher. Das gibt Ihnen auch die Möglichkeit, WMI-Schnittstellen mit der integrierten Funktionalität von Windows-PowerShell zu kombinieren.

Klassen für die Terminalserver-Konfiguration

In Windows Server 2008 gibt es keine neuen Klassen für die Terminalserver-Konfiguration. Wie aber Tabelle 1.4 zeigt, sind einige Änderungen an den vorhandenen Klassen zu verzeichnen. Speziell gibt es jetzt die Möglichkeit, die Quelle der Konfigurationseinstellung zu ermitteln – der Server selbst oder eine darauf angewendete Gruppenrichtlinie. Die Klasse *SessionDirectory* besitzt zudem in Windows Server 2008 weit mehr Methoden und Eigenschaften als in Windows Server 2003.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

WMI-Klasse	Beschreibung	Änderungen seit Windows Server 2003
Win32_TerminalService	Die Klasse *Win32_TerminalService* ist eine Subklasse der Klasse *Win32_Service* und erbt alle ihre Eigenschaften und Methoden. Außerdem stellt *Win32_TerminalService* die Eigenschaft *Element* der Zuordnung *Win32_TerminalServiceToSetting* dar.	Keine
Win32_TSSessionDirectory	Definiert die Konfiguration für *Win32_TSSessionDirectorySetting*, einschließlich der Eigenschaften wie z. B. *SessionDirectory store* und *Cluster Name*.	Diese Klasse hatte in Windows Server 2003 nicht viel zu tun, sodass es viele Änderungen seit WS03 gibt. Dazu gehören die neuen Methoden *GetCurrentRedirectableAddresses*, *SetCurrentRedirectableAddresses*, *GetRedirectableAddresses*, *PingSessionDirectory*, *SetLoadBalancingState* und *SetServerWeight*. Alle dazu gehörenden Eigenschaften sind ebenfalls neu in Windows Server 2008.
Win32_TerminalServiceSetting	Definiert die Konfiguration für *TerminalServerSetting*, einschließlich der Eigenschaften wie z. B. *TerminalServerMode*, *Licensing* und *ActiveDesktop*. Daneben gibt es Eigenschaften, die sich auf Berechtigungen, Löschen temporärer Ordner und temporäre Verzeichnisse für Sitzungen beziehen.	Diese Klasse besitzt mehrere neue Eigenschaften: *LimitedUserSessions*, *PossibleLicensingTypes*, *SessionBrokerDrainMode* und mehrere Eigenschaften für die Richtlinienquelle, um zu ermitteln, ob eine bestimmte Konfiguration von einer Gruppenrichtlinie oder einer lokalen Serverkonfiguration stammt. Außerdem werden mehrere neue Methoden unterstützt, u. a. *CreateWinStation*, *PingLicenseServer* und *UpdateDirectConnectLicenseServer*.
Win32_Terminal	Verbindet eine *TerminalSetting* und ihre verschiedenen Klassen zur Konfigurationseinstellung in dieser Tabelle, wie z. B.: *General*, *Logon*, *Session*, *Environment*, *Remote Control*, *Client*, *Network Adapter* und *Permission*.	Die Methoden *Create* und *Delete* für diese Klasse sind neu in Windows Server 2008.
Win32_TSGeneralSetting	Definiert Eigenschaften wie z. B. *Protocol*, *Transport*, *Comment*, *Windows Authentication* und *Encryption Level*.	Windows Server 2003 SP1 hat die Unterstützung für die Methode *SetSecurityLayer* hinzugefügt. Die Unterstützung für *SetUserAuthenticationRequired* ist neu in Windows Server 2008.
Win32_TSLogonSetting	Definiert Eigenschaften wie z. B. *ClientLogonInfoPolicy*, *UserName*, *Domain* und *Password*.	In Windows Server 2003 wird *ClientLogonInfoPolicy* nicht verwendet, jedoch in Windows Server 2008. Mehrere Eigenschaften für die Richtlinienquelle, um zu ermitteln, ob eine bestimmte Konfiguration von einer Gruppenrichtlinie oder einer lokalen Serverkonfiguration stammt, sind ebenfalls neu in Windows Server 2008.
Win32_TSSessionSetting	Definiert Eigenschaften wie z. B. die Zeitüberschreitungsrichtlinie für Verbindungen und Zeitlimits für aktivierte, getrennte und Leerlaufsitzungen.	Mehrere Eigenschaften für die Richtlinienquelle, um zu ermitteln, ob eine bestimmte Konfiguration von einer Gruppenrichtlinie oder einer lokalen Serverkonfiguration stammt, sind neu in Windows Server 2008. ▶

WMI-Klasse	Beschreibung	Änderungen seit Windows Server 2003
Win32_TSEnvironmentSetting	Definiert Eigenschaften wie z. B. Programmrichtlinie, Programmpfad, Arbeitsverzeichnis und Hintergrund des Clients.	Mehrere Eigenschaften für die Richtlinienquelle, um zu ermitteln, ob eine bestimmte Konfiguration von einer Gruppenrichtlinie oder einer lokalen Serverkonfiguration stammt, sind neu in Windows Server 2008.
Win32_TSRemoteControlSetting	Definiert Eigenschaften wie z. B. die Remoteüberwachungsrichtlinie und die Steuerungsebene.	Mehrere Eigenschaften für die Richtlinienquelle, um zu ermitteln, ob eine bestimmte Konfiguration von einer Gruppenrichtlinie oder einer lokalen Serverkonfiguration stammt, sind neu in Windows Server 2008.
Win32_TSClientSetting	Definiert Eigenschaften wie z. B. die Verbindungsrichtlinie, Windows-Druckerzuordnung, PNP-Umleitung und COM-Anschlusszuordnung.	Die Eigenschaft *PNPRedirection* ist neu in Windows Server 2008. Mehrere Eigenschaften für die Richtlinienquelle, um zu ermitteln, ob eine bestimmte Konfiguration von einer Gruppenrichtlinie oder einer lokalen Serverkonfiguration stammt, sind ebenfalls neu in Windows Server 2008.
Win32_TSNetworkAdapterSetting	Definiert Eigenschaften wie z. B. LAN-Adapter und maximale Anzahl von Verbindungen.	In Windows Server 2008 stehen jetzt einige Informationen über Netzwerkadapter zur Verfügung, u. a. *DeviceIDList*, *NetworkAdapterList* und *NetworkAdapterLanaID*. Ebenfalls neu ist die Eigenschaft, mit der sich die Richtlinienquelle für die maximale Anzahl der Verbindungen ermitteln lässt.
Win32_TSNetworkAdapterListSetting	Listet basierend auf Terminalprotokoll und Transport die Netzwerkadapter auf, die für *Win32_Terminal* konfigurierbar sind. U. a. gibt es folgende Eigenschaften: *TerminalProtocol*, *Transport*, *NetworkAdapterID* und *Description*.	Keine
Win32_TSPermissionsSetting	Repräsentiert eine Zuordnung zwischen einem *Win32_Terminal* und seinen Konfigurationseinstellungen (*Win32_TSAccount*). Enthält Eigenschaften für das Hinzufügen von Konten zu definierten Berechtigungssätzen und das Wiederherstellen von Berechtigungen.	Die Eigenschaften *StringSecurityDescriptor* und *DenyAdminPermissionForCustomization* sind neu für Windows Server 2008. Ebenfalls neu ist eine Eigenschaft für die Richtlinienquelle, um zu ermitteln, ob eine bestimmte Konfiguration von einer Gruppenrichtlinie oder einer lokalen Serverkonfiguration stammt.
Win32_TSAccount	Definiert Eigenschaften wie SID, zugelassene und verweigerte Berechtigungen.	Keine

Tabelle 1.4 Klassen für die Terminaldienstekonfiguration in Windows Server 2008 und Änderungen gegenüber Windows Server 2003

Klassen für Terminaldienste-Sitzungsbroker

Obwohl Terminaldienste-Sitzungsbroker einen neuen Namen und neue Funktionalität in Windows Server 2008 bekommen hat, sind die WMI-Schnittstellen, die Tabelle 1.5 beschreibt, ähnlich denen für das Sitzungsverzeichnis in Windows Server 2003. Als Unterschied fällt die Nomenklatur ins Auge. Zum Beispiel

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

wird in Windows Server 2003 eine Sammlung von Servern als *Cluster* bezeichnet, während in Windows Server 2008 eine Sammlung gleichartiger Server, die durch einen Sitzungsbroker verwaltet werden, *Farm* heißt. Außerdem werden einige Eigenschaften, die in *Win32_SessionDirectoryServer* definiert sind, in Windows Server 2003 nicht unterstützt.

HINWEIS Wenn in diesem Buch von einer *Farm* die Rede ist, meinen wir eine Gruppe von *gleichartigen* Terminalservern mit Lastenausgleich. Auch wenn sie sich in Bezug auf die Hardware geringfügig unterscheiden können, wird bei allen Terminalservern in einer Farm vorausgesetzt, dass sie die gleiche Konfiguration und den gleichen Anwendungssatz haben.

Klasse	Beschreibung	Funktionalität
Win32_SessionDirectoryCluster	Stellt eine Farm in Terminaldienste-Sitzungsbroker dar.	Liefert den Namen der Terminalserver-Farm, die Anzahl der dazu gehörenden Server und ob sich die Farm im Modus mit nur einer Sitzung befindet (d.h. pro Benutzer nur eine einzige Sitzung möglich ist, sodass der Benutzer mit derselben Sitzung verbunden wird, wenn die Sitzung getrennt wurde und der Benutzer sich erneut verbinden möchte).
Win32_SessionDirectoryServer	Stellt einen Terminaldienste-Sitzungsbroker-Server dar.	Beschreibt den aktuellen Zustand des Sitzungsbrokers einschließlich Name, IP-Adresse, Anzahl der Sitzungen mit ausstehenden erneuten Verbindungen, Anzahl der Sitzungen und Servergewichtung.
Win32_SessionDirectorySession	Stellt eine Terminaldienste-Sitzungsbroker-Sitzung dar.	Beschreibt die Sitzung an sich einschließlich Sitzungs-ID, Benutzername und Domänenname des Endbenutzers mit der Verbindung, der Uhrzeit, wann die Sitzung erstellt (und falls zutreffend getrennt) wurde, und das Erscheinungsbild der Sitzung (Farbtiefe und Auflösung).

Tabelle 1.5 WMI-Schnittstellen für Sitzungsbroker in Windows Server 2008

Die übrigen Klassen sind alle neu in Windows Server 2008.

HINWEIS Es stehen auch WTS-Schnittstellen zur Verfügung, um die Funktionalität von Terminaldienste-Sitzungsbroker zu erweitern. Allerdings sind diese nur nützlich, wenn Sie Erweiterungen zu Terminaldienste-Sitzungsbroker erstellen (und nicht nur die vorhandene Funktionalität verwalten) möchten. Weitere Details finden Sie unter *http://msdn.microsoft.com/en-us/library/cc644953(VS.85).aspx*.

Klassen für Terminaldienstegateway

Mit den in Tabelle 1.6 gezeigten Klassen steuern Sie die Verbindungen, Richtlinien und Terminaldienstegateway-Konfigurationen und -Beziehungen. Die Spalte *Funktionalität* listet nicht sämtliche Eigenschaften und Methoden auf, gibt aber repräsentative Beispiele an, wofür die betreffende Klasse vorgesehen ist.

Klasse	Beschreibung	Funktionalität
Win32_TSGatewayConnection	Stellt eine Verbindung von einem Clientcomputer zu einem Terminaldienste-Gatewayserver dar.	Überprüft Verbindungsstatus und beendet selektiv Sitzungen. Identifiziert Informationen über die Verbindung, einschließlich wie lange sie aktiv ist und mit welcher Farm oder welchem Server der Endbenutzer verbunden ist.
Win32_TSGatewayConnectionAuthorizationPolicy	Stellt eine Terminaldienste-Verbindungsautorisierungsrichtlinie (TS-CAP) dar.	Definiert die Benutzergruppen, die Verbindungen herstellen dürfen, und die ihnen offen stehenden Autorisierungsmethoden (z.B. Smartcard, Kennwort). Definiert außerdem die Einschränkungen für die Verbindung, beispielsweise ob Zwischenablagezuordnung erlaubt ist. Da ein Terminaldienstegateway über mehrere Verbindungsautorisierungsrichtlinien verfügen kann, ermöglicht Ihnen diese Klasse auch, den TS-CAPs eindeutige Namen zuzuweisen.
Win32_TSGatewayLoadBalancer	Stellt einen Satz von Terminaldienste-Gatewayservern mit Lastenausgleich dar.	Verwaltet die Terminaldienstegateway-Lastenausgleichmitgliedschaft. Erlaubt es, Lastenausgleichmitglieder hinzuzufügen, zu löschen oder abzufragen.
Win32_TSGatewayRADIUSServer	Beschreibt und verwaltet einen RADIUS-Server, der die Verbindungsautorisierungsrichtlinien verwaltet.	Ändert Priorität oder Name des RADIUS-Servers, bearbeitet gemeinsame geheime Informationen.
Win32_TSGatewayResourceAuthorizationPolicy	Stellt eine Terminaldienste-Ressourcenautorisierungsrichtlinie (TS-RAP) dar.	Bearbeitet den Namen oder die Beschreibung einer TS RAP. Fügt der TS RAP Benutzergruppen hinzu oder löscht sie aus der TS RAP. Ermöglicht Ihnen außerdem, neue TS RAPs zu erstellen oder sie zu löschen.
Win32_TSGatewayResourceGroup	Stellt eine Ressourcengruppe (einen Satz von Computernamen, zu dem jeder mit der entsprechenden TS RAP zugreifen kann) dar.	Bearbeitet den Namen oder die Beschreibung einer Ressourcengruppe. Fügt einer Ressourcengruppe Ressourcen hinzu oder löscht sie aus der Gruppe.
Win32_TSGatewayServer	Verwendet für spezifische Operationen von Terminaldienste-Gatewayserver, wie zum Beispiel das Importieren und Exportieren von Konfigurationen oder das Erstellen von Zertifikaten.	Importiert oder exportiert Konfigurationseinstellungen, die in der XML-Datei gespeichert sind, oder erstellt ein selbstsigniertes Zertifikat.
Win32_TSGatewayServerSettings	Stellt die Konfiguration eines Terminaldienste-Gatewayservers dar.	Konfiguriert Ereignisprotokollierung, wenn ein zentraler CAP-Server eine Richtlinie festlegt, wenn eine Integritätsanweisung (vom Client, der eine Verbindung herzustellen versucht) angefordert wird, und die maximale Anzahl von erforderlichen Verbindungen.

Tabelle 1.6 WMI-Klassen für Terminaldienstegateway

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

Klassen für Terminaldienstelizenzierung

Obwohl die Rolle *Terminaldienstelizenzierung* in Windows Server 2008 nicht neu ist, gab es die Klassen, die zu dieser Rolle gehören und die in Tabelle 1.7 beschrieben sind, noch nicht in Windows Server 2003.

HINWEIS Beachten Sie, dass TS-CALs pro Gerät und pro Benutzer getrennt verwaltet werden.

Klasse	Beschreibung	Funktionalität
Win32_TSIssuedLicense	Beschreibt Instanzen von TS-CALs (pro Gerät), die von einem Terminaldienste-Lizenzserver ausgestellt werden.	Sperrt eine TS-CAL oder liefert Informationen über ihr Ablaufdatum, die *KeyPackID*, den Lizenztyp (aktiv, temporär, gesperrt usw.) und stellt Bezeichner für den Computer aus, dem sie zugewiesen ist.
Win32_TSLicenseKeyPack	Stellt Methoden und Eigenschaften bereit, um Terminaldienste-Lizenzschlüsselpakete anzuzeigen und zu installieren.	Installiert verschiedene Typen von Lizenzschlüsselpaketen und ermittelt die Anzahl der TS-CALs im Paket, die Produktversion der TS-CAL (zurück zu Windows 2000-TS-CALs) und den Typ (pro Benutzer oder pro Gerät).
Win32_TSLicenseReport	Zeigt die Verwendung von TS-CALs (pro Benutzer) für diesen Lizenzserver an.	Erzeugt und verwaltet Verwendungsberichte von TS-CALs (pro Benutzer). Die mit WMI erzeugten Berichte erscheinen im Terminaldienstelizenzierungs-Manager.
Win32_TSLicenseReportEntry	Stellt Details einer ausgegebenen TS-CAL (pro Benutzer) bereit.	Liefert Details über das Ablaufdatum einer TS-CAL (pro Benutzer).
Win32_TSLicenseServer	Stellt Methoden und Eigenschaften bereit, um einen Terminaldienste-Lizenzserver anzuzeigen und zu konfigurieren.	Legt die Konfigurationsinformationen für die Aktivierung eines Lizenzservers fest (einschließlich der Firmeninformationen). Diese Klasse umfasst auch Methoden, um einen Lizenzserver zu aktivieren, zu deaktivieren und erneut zu aktivieren

Tabelle 1.7 WMI-Klassen für Terminaldienstelizenzierung in Windows Server 2008

HINWEIS Auch wenn sich mit der Klasse *Win32_TSLicenseReportEntry* ermitteln lässt, zu welcher Version von Terminalserver die Verbindung mit einer TS-CAL (pro Benutzer) hergestellt werden kann und Windows 2000 Server ein gültiger Rückgabewert für diese Eigenschaft ist, gibt es keine TS-CALs (pro Benutzer) für Terminaldienste von Windows 2000 Server.

Klassen für Terminaldienste-RemoteApp

Die RemoteApp-Programme werden getrennt von den Terminalserver-Einstellungen verwaltet, selbst wenn der Terminalserver die RemoteApp-Programme verfügbar macht. Tabelle 1.8 beschreibt deren WMI-APIs.

Klasse	Beschreibung	Funktionalität
Win32_RemoteAppChangeEvent	Stellt eine Änderung an den RemoteApp-Einstellungen auf dem Terminalserver dar.	Diese Klasse erbt von der Systemklasse *ExtrinsicEvent*, definiert aber keine zusätzlichen Methoden und Eigenschaften.
Win32_TSPublishedApplicationList	Stellt die Liste der Programme dar, die in der RemoteApp-Programmliste auf einem Terminalserver enthalten sind.	Diese Klasse definiert keine Methoden. Die Eigenschaften der Klasse geben an, ob der Terminalserver Benutzern erlaubt, die Verbindung mit beliebigen der darauf installierten Anwendungen zu beginnen oder nur mit den Anwendungen, die der Administrator als veröffentlichte Anwendungen gekennzeichnet und sie der Zulassungsliste hinzugefügt hat.
Win32_TSPublishedApplication	Definiert die Anwendungen, die für Remoteverwendung über Terminaldienste-RemoteApp verfügbar gemacht wurden.	Listet die Anwendungen auf, die auf dem Terminalserver veröffentlicht sind, und liefert Details wie z. B. Pfad (tatsächlich und virtuell), Symbol, ob die Anwendung in Terminaldienste-Webzugriff erscheint und alle Einschränkungen oder Anforderungen für die Verwendung von Befehlszeilenoptionen, um die Anwendung zu starten.
Win32_TSRemoteDesktop	Beschreibt die Remotedesktopverbindung zum Terminalserver, die über Terminaldienste-Webzugriff verfügbar gemacht werden kann.	Liefert die Namen, Symbole und Pfade der autorisierten Anwendungen, um sie in Terminaldienste-Webzugriff anzuzeigen.
Win32_TSDeploymentSettings	Definiert die Bereitstellungseinstellungen für RemoteApp-Programme.	
Win32_TSStartMenuApplication	Beschreibt die Anwendungen, die im Menü *Start* eines Terminalservers aufgeführt sind.	
Win32_TSApplicationFileExtensions	Beschreibt die Dateierweiterungen, die von einer Anwendung auf einem Terminalserver verarbeitet werden.	
Win32_TSExpandEnvironmentVariables	Erweitert systemdefinierte Umgebungsvariablen.	

Tabelle 1.8 WMI-Schnittstellen für RemoteApps

HINWEIS *Win32_TSPublishedApplicationList* wird nur auf das ursprüngliche Programm angewendet, das ein Benutzer auf einem Terminalserver ausführt. Wenn die Verbindung eingerichtet ist, kann der Endbenutzer – wenn nicht anderweitig verhindert – jede Anwendung ausführen, die auf dem Terminalserver installiert ist.

Zusammenfassung

Dieses Kapitel hat Sie in Windows Server 2008 Terminaldienste eingeführt. Damit sollten Sie jetzt verstehen, wie sich diese Rolle entwickelt hat, seit sie vor 10 Jahren zum Bestandteil von Windows geworden ist, und wofür Terminaldienste verwendet werden. Weiterhin wurden die neuen Geschäftsszenarios behandelt, die Windows Server 2008 Terminaldienste jetzt unterstützen, und die Rollen, die diese neuen Geschäftsszenarios unterstützen und wie sie zusammenwirken. Außerdem haben Sie nun einen Überblick über die anderen Windows-Rollen, die die Funktionalität von Terminaldiensten direkt unterstützen. Schließlich wurde dargestellt, wie Terminaldienste aufgebaut sind, um nicht nur ein Featureset zu sein, sondern eine Plattform, auf der ISVs und Berater zugeschnittene Projekte und Skripts entwickeln können. Dabei wurde auch erläutert, wie sich diese Plattform gegenüber der in Windows Server 2003 weiterentwickelt hat. Das nächste Kapitel baut auf den Kenntnissen dieses Rollensatzes auf und beschäftigt sich mit der Planung einer Terminalserverumgebung.

Zusätzliche Ressourcen

Dieses Kapitel hat eine Anzahl von Konzepten eingeführt, die wir im weiteren Verlauf dieses Buchs vertiefen werden.

- Weitere Informationen zur Speicherverwendung in Terminalservern finden Sie in Kapitel 2.
- Mit der Kernrolle von Terminalserver und der TS-Lizenzierung beschäftigt sich Kapitel 3.
- Drucken mit Terminaldiensten ist Thema von Kapitel 5.
- Kapitel 6 geht ausführlich auf Terminaldienste-Webzugriff ein.
- In Kapitel 7 erfahren Sie mehr zu Terminaldienste-Sitzungsbroker.
- Ebenfalls in Kapitel 7 wird das Thema Terminaldienstegateway behandelt.

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)

Christa Anderson, Kristin L. Griffin mit dem Microsoft Presentation Hosted Desktop Virtualization Team:
Microsoft Windows Server 2008 Terminaldienste, Microsoft Press 2009 (ISBN 978-3-86645-663-1)