Microsoft

Windows Server® 2008 R2: Usługi pulpitu zdalnego *Resource Kit*

Christa Anderson i Kristin L. Griffin
przy współpracy Remote Desktop Virtualization Team

Przekład:
Marek Włodarz

APN Promise
Warszawa 2011

Windows Server® 2008 R2: Usługi pulpitu zdalnego Resource Kit

Authorized Polish translation of English edition of
Windows Server® 2008 Remote Desktop Services Resource Kit
ISBN: 978-0-7356-2737-6

APN PROMISE SA, ul. Kryniczna 2, 03-934 Warszawa
tel. +48 22 35 51 600, fax +48 22 35 51 699
e-mail: mspress@promise.pl

ISBN: 978-83-7541-081-5
Przekład: Marek Włodarz
Korekta: Ewa Swędrowska
Skład i łamanie: MAWart Marek Włodarz

Spis treści

Podziękowania

Książka ta nie jest jedynie dziełem dwóch osób. Jesteśmy winne wiele podziękowań za połączone wysiłki wielu ludzi z firmy Microsoft, wspaniałego zespołu redakcyjnego oraz całej społeczności (co powiedziawszy, wszystkie błędy w tej książce są wyłączną winą autorek).

Jedną z najlepszych rzeczy, jakie wynikają z pracy w firmie Microsoft, jest to, że pracuje tu bardzo wielu błyskotliwych (i pomocnych) ludzi – wszystkim tym ludziom jesteśmy wdzięczne za wskazówki i pomoc. W różnych miejscach tej książki znaleźć można ramki zatytułowane „Wprost ze źródła", które napisali członkowie zespołu projektowego i inni pracownicy Microsoft. Dziękować musimy też członkom zespołu, którzy poświęcili czas na wyjaśnienia szczegółów. Z zespołu Remote Desktop Virtualization (RDV) podziękowania należą się następującym osobom: Niraj Agarwala, James Baker, Ara Bernardi, Tad Brockway, Vikash Bucha, Yuvraj Budhraja, Hammad Butt, Rommy Channe, Munindra Das, Silvia Doomra, Samim Erdogan, Rajesh Ganta, Costin Hagiu, Al Henriquez, Travis Howe, Olga Ivanova, Gopikrishna Kannan, Sergey Kuzin, Rob Leitman, Raghu Lingampally, Meher Malakapalli, Benjamin Meister, Ranjana Rathinam, Rajesh Ravindranath, Ray Reskusich, Sriram Sampath, Bhaskar Swarna oraz Janani Venkateswaran. Zaangażowane były też osoby z innych zespołów, w tym Kyle Beck, Jeff Heatton, Michael Kleef, Timothy Newton, Mark Russinovich, Tom Shinder, Makarand Patwardhan, Bohdan Velushchak, Paul Volosen i Jon Wojan. Chcemy też podziękować menedżerowi Christy, Ashwinowi Palekar, za jego poparcie podczas realizacji tego projektu.

Wiedza dotycząca RDS nie jest tylko domeną pracowników Microsoft. Wielu MVP w dziedzinie pulpitu zdalnego, jak również w innych dyscyplinach, przyczyniło się do powstania ramek „Wprost do źródła" i wyjaśniło zależności w powiązanych technikach. Podziękowania chciałybyśmy złożyć następującym osobom: Janique Carbone, Brian Ehlert, Ross Harvey, Helge Klein, Russo Kaufmann, Shay Levy, Brian Madden, Patrick Rouse, Greg Shields, Michael Smith oraz Mitch Tulloch.

Na koniec chcemy podziękować naszym przyjaciołom i rodzinom za ich wsparcie podczas tego wielkiego wyzwania. Nic nie dałybyśmy rady zrobić bez was.

I obiecujemy, że teraz będziemy mówić o czymś innym...

Wprowadzenie

Witamy w *Windows Server 2008 R2: Usługi pulpitu zdalnego Resource Kit*, szczegółowym źródle informacji technicznych na temat planowania, wdrażania i utrzymywania Microsoft *Remote Desktop Services* (Usług pulpitu zdalnego), czyli RDS[1]. Ponieważ niektóre funkcje RDS są zupełnie nowe, dostępne dopiero od tej wersji systemu operacyjnego, książka powinna być użyteczna nie tylko dla tych, którzy dopiero zaczynają przygodę z RDS, ale i dla tych, którzy używali *Terminal Services* (co jest wcześniejszą nazwą tego samego rozwiązania) we wcześniejszych wersjach Microsoft Windows.

Książka przedstawia usprawnienia wprowadzone w RDS w Windows Server 2008 R2. Łączy leżące u podstaw koncepcje architektoniczne z praktycznymi instrukcjami, które pozwolą skonfigurować działający ekosystem RDS, zrozumieć, *dlaczego* on działa, i dać pewne wskazówki, jak go naprawić, gdyby przestał. Znajdziemy tu też szczegółowe informacje i zorientowane na zadania wskazówki na temat zarządzania wszelkimi aspektami RDS, takie jak wdrażanie serwerów RD Session Host, integrowanie roli RDS z innymi kluczowymi częściami systemu operacyjnego Windows Server 2008 R2 i rozszerzanie zasięgu RDS poza granice sieci korporacyjnej. Na koniec dołączony do książki dysk CD zawiera dodatkowe narzędzia oraz dokumentację, która może być pomocna przy zarządzaniu i rozwiązywaniu problemów z usługami roli RDS. Choć wspominamy o niektórych narzędziach innych firm, książka jest zasadniczo poświęcona utrzymywaniu RDS przy użyciu jedynie tych narzędzi, które znajdziemy w samym systemie operacyjnym. Mówiąc inaczej, każdy może zrobić każdą przedstawioną tu rzecz, używając *tylko* Windows Server 2008 R2. Nie wchodzimy też w szczegółowe omówienia narzędzi innych firm, których wiele osób używa do pracy z Remote Desktop Services. Na przykład wiele osób obsługujących bardzo złożone wdrożenia RDS wykorzystuje oprogramowanie zarządzające firm Citrix lub Quest, czy też innych firm partnerskich, ale nie omawiamy ich tu, gdyż nie są one dołączone do systemu operacyjnego.

Na dołączonym nośniku Lista firm tworzących produkty uzupełniające lub rozszerzające rozwiązania pulpitu zdalnego w Windows Server 2008 R2 znajduje się na stronie partnerów zespołu pod adresem *http://www.microsoft.com/windowsserver2008/en/us/rds-partners.aspx*.

1 Dla zachowania czytelności w całej książce stosowane są akronimy pochodzące od angielskich nazw poszczególnych ról, usług bądź technologii. Zestawienie tych akronimów wraz z ich rozwinięciem i polskim odpowiednikiem znajduje się na końcu Wprowadzenia (wszystkie przypisy pochodzą od tłumacza).

Co nowego w Windows Server 2008 R2?

Remote Desktop Services (Usługi pulpitu zdalnego) w systemie Windows Server 2008 R2 zawierają wiele usprawnień, zarówno takich, które pojawiły się już w Windows Server 2008, jak i takich, które stanowiły reakcję na żądania użytkowników. Chcecie wbudowanej obsługi VDI? Proszę bardzo, została dodana do RD Connection Broker. Chcecie mniej razy wpisywać hasła, filtrować zabezpieczenia, uproszczenia wyszukiwania dostępnych aplikacji i maszyn wirtualnych? Znajdziecie to w nowej wersji RD Web Access. Chcecie rozwiązać problemy odkryte przez mechanizm Network Access Policies (NAP), a nie tylko odciąć tych ludzi od sieci? Jest to możliwe w nowym wydaniu RD Gateway. Potrzebna jest lepsza zgodność aplikacji? Sprawdźcie funkcje wirtualizacji adresu IP dla sesji oraz dynamicznego przydzielania procesora, aktywnie zabezpieczającej przed zawłaszczeniem całej mocy procesora przez jedną z sesji. Nie chcecie ciągle instalować sterowników drukarek, czy to na serwerach sesji, czy maszynach wirtualnych? Easy Print działa obecnie dla obu opcji dostępu zdalnego.

Oto krótki przegląd nowych funkcji dodanych do starszego modelu serwera terminali dla tych, którzy przechodzą bezpośrednio do Windows Server 2008 R2 z Windows Server 2003.

Uproszczone dostarczanie i wyświetlanie aplikacji

Terminal Services (Usługi terminalowe) w systemie Windows Server 2003 prezentowały wszystkie zdalne aplikacje na pulpicie zdalnym, całkowicie oddzielając od siebie programy lokalne i zdalne. Programy RemoteApp (wprowadzone w systemie Windows Server 2008) są uruchamiane na serwerze, ale integrują się z lokalnym pulpitem w taki sposób, że wyglądają tak, jakby były wykonywane lokalnie.

Aplikacje nie tylko są lepiej zintegrowane z lokalnym pulpitem, ale są również łatwiejsze do odnalezienia i dystrybucji, tym samym ułatwiając wsparcie w dużych, rozbudowanych wdrożeniach. Jednym z problemów, które nieodłącznie towarzyszą rozwiązaniom zdalnego dostępu, jest dostarczenie użytkownikom możliwie kompletnej i aktualnej listy zasobów. Staje się to jeszcze bardziej prawdziwe, gdy zapewniamy dostęp do indywidualnych aplikacji, a nie do pełnego pulpitu. Przy użyciu rozwiązania RD Web Access można prezentować łącza do poszczególnych aplikacji lub pełnych pulpitów i mieć pewność, że łącza te zawsze będą aktualne. W systemie Windows Server 2008 R2 witryna RD Web Access może przedstawiać programy RemoteApp z więcej niż jednej farmy serwerów, a także z maszyn wirtualnych. Może też wykorzystywać filtrowanie zabezpieczeń, zatem możemy utrzymywać pojedyncze, zbiorcze źródło wszystkich zasobów zdalnych, ale użytkownicy będą widzieli tylko te zasoby, których powinni używać.

Ulepszona obsługa farm serwerów

Usługa Session Directory w systemie Windows Server 2003 oferowała coś, co można nazwać „początkiem" obsługi farmy, ale była dostępna tylko w wydaniu Enterprise i nie zawierała żadnego równoważenia obciążeń – jedynie pamiętała, gdzie poszło które połączenie. W systemie Windows Server 2008 R2 komponent RD Connection Broker jest dostępny w edycji Standard, wspiera równoważenie obciążeń i może przekierowywać obciążenia zarówno do serwerów sesji, jak i maszyn wirtualnych.

Bezpieczny dostęp z Internetu

Jedną z kluczowych korzyści usług pulpitu zdalnego jest możliwość obsługi pracowników ruchomych. Przy pracy nad tą książką pomagał nam wspaniały (i niebywale ruchliwy) redaktor techniczny, zarazem MVP w dziedzinie RDS, Alex Juschin. Oto jego opis, jak korzystał z Remote Desktop Services podczas wykonywania swojej części pracy.

> *W swojej książce możecie zaznaczyć, że przeglądałem ją z niemal dowolnych miejsc na świecie, używając protokołu RDP do łączenia się z moim domowym komputerem w Dublinie via 3G lub WiFi . Pracowałem siedząc w pierogarni w Polsce, w niedogrzanym hotelu na Łotwie, jadąc luksusowym autokarem w Estonii, na promie do Anglii, w pubie w Irlandii, w pociągu jadącym na wybrzeże z Belfastu, smakując wino we Francji, siedząc w miłej knajpce na wyspie Jersey, jedząc belgijską czekoladę w Brukseli, w samolocie do Niemiec, na ławce z przepięknym widokiem w Zurichu, w kawiarni koło muru berlińskiego, w więzieniu w Finlandi (ok, to jest hotel, ale kiedyś był więzieniem) i na najwyższym szczycie Niemiec (Zugspitze).*

W systemie Windows Server 2003 Terminal Services nie obsługiwały bezpiecznego dostępu z Internetu z wyjątkiem stosowania wirtualnych sieci prywatnych. W systemie Windows Server 2008 R2 Remote Desktop Services obsługują łączność przy użyciu Secure Sockets Layer (SSL) via RD Gateway. Mechanizm ten pozwala zdefiniować odmienne reguły dla lokalnego i zewnętrznego dostępu, nie wymagając żadnego konfigurowania po stronie klienta. Wprowadzony w systemie Windows Server 2008 mechanizm RD Gateway został w wersji R2 rozszerzony o wymuszanie ustawień przekierowania urządzeń i zasobów zdefiniowanych na bramie i wspiera rozwiązania naprawcze NAP.

Prostsze i szersze przekierowanie urządzeń

RDS są zaprojektowane przy założeniu, że wiele osób będzie pracowało zdalnie z komputerów dysponujących własnymi, lokalnymi zasobami i że ci użytkownicy nie będą chcieli być odcięci od tego sprzętu, gdy będą pracowali w sesji zdalnej lub na maszynie wirtualnej. Zakłada się też, że administratorzy serwerów nie chcą spędzać więcej czasu, niż to niezbędnie konieczne, aby zapewnić dostępność tych zasobów.

Choć przekierowywanie drukarek, znane z wcześniejszych wersji Terminal Services, nadal działa tak samo, mechanizm *Easy Print* (Łatwe drukowanie), wprowadzone w systemie Windows Server 2008, znacząco upraszcza korzystanie z drukarki lokalnej w sesji zdalnej. Zamiast żądać od administratorów, aby instalowali potrzebne sterowniki drukarek na serwerze, Easy Print umożliwia przekierowanym drukarkom korzystanie ze sterowników już zainstalowanych na komputerach klienckich. W systemie Windows Server 2008 R2 mechanizm Easy Print działa z jeszcze większą liczbą typów drukarek i jest dostępny zarówno w sesjach pulpitu zdalnego, jak i przy korzystaniu z maszyn wirtualnych.

Częścią bogatego środowiska roboczego jest wykorzystanie lokalnych urządzeń. Wsparcie dla lokalnych urządzeń zostało rozszerzone poprzez Plug and Play Device Redirection Framework, wprowadzone w systemie Windows Server 2008.

Uproszczone zarządzanie licencjami

Licencjonowanie na użytkownika zostało wprowadzone w Windows Server 2003, jednak nie był dostępny żaden mechanizm śledzenia, zatem nie można było łatwo sprawdzić, czy firma jest w zgodzie z porozumieniem licencyjnym. Windows Server 2008 R2 pozwala śledzić wykorzystanie licencji RDS CAL na użytkownika. Dodatkowo pojawiła się funkcja *Licensing Diagnostics* (Diagnostyka licencjonowania), która pomaga na rozwiązywaniu problemów dotyczących licencji. Serwery licencji systemu Windows Server 2008 R2 pozwalają na migrowanie licencji z jednego serwera na inny bez angażowania Microsoft Clearinghouse. Może to być wykonane nawet wtedy, gdy serwer licencji jest poza zasięgiem lub całkowicie wyłączony.

To tylko cząstkowa lista nowych funkcji – rozdział 1, „Wprowadzenie do RDS", zawiera szersze omówienie nowych funkcji Remote Desktop Services w Windows Server 2008 R2, zaś reszta książki pokazuje, jak z nich korzystać. Jednak te wymienione pokazują, jak bardzo rola ta się rozwinęła pod względem środowiska użytkowników i możliwości zarządzania.

Jak zbudowana jest ta książka

Celem, który przyświecał nam przy pisaniu tej książki, było zapewnienie pomocy w budowania infrastruktury zdalnego pulpitu, zawierającej zarówno farmy serwerów RD Session Host, jak i zbiorcze i osobiste maszyny wirtualne, przy jednoczesnym zrozumieniu szerszego kontekstu warunków, w których RDS stają się użyteczne, jak działają, i jak wygląda Windows Server 2008 R2 w porównaniu do wcześniejszych wersji. Książka zawiera dwanaście rozdziałów:

- Rozdział 1, „Wprowadzenie do RDS", wyjaśnia, skąd wzięły się RDS i jak ewoluowały jako platforma, jakie są nowe funkcje najnowszego wydania i co można osiągnąć przy użyciu tej wersji produktu. Pokazuje również, jak inne usługi wspierają RDS.
- Rozdział 2, „Kluczowe koncepcje architektury RDS", zagłębia się w szczegóły budowy RDS i odpowiadające im elementy Windows Server 2008 R2. Pokazuje też, jak można określić wymagania sprzętowe i programowe.
- Rozdział 3, „Wdrażanie pojedynczego serwera RD Session Host", pokazuje, jak działają serwery RD Session Host i jak zainstalować i skonfigurować tę usługę roli.
- Rozdział 4, „Wdrażanie pojedynczego serwera RD Virtualization Host", wyjaśnia, czym jest VDI, jak działa Microsoft VDI i jak zainstalować i skonfigurować serwer RD Virtualization Host oraz wspierające role i usługi.
- Rozdział 5, „Zarządzanie danymi użytkowników we wdrożeniu RDS", omawia różne typy profili występujące w środowisku RDS oraz jak wdrażać różne wersje profili użytkowników i rozwiązywać problemy z profilami i przekierowywaniem folderów.
- Rozdział 6, „Konfigurowanie środowiska użytkowników", pokazuje, jak działa przekierowywanie urządzeń, jak budować dobre środowisko użytkownika w sesji zdalnej i konfigurować drukowanie.

- Rozdział 7, „Formowanie i zabezpieczanie środowiska użytkownika”, wyjaśnia, dlaczego należy zabezpieczyć środowisko RDS i ja można to zrobić, a ponadto pokazuje, jak można zapewnić zdalną pomoc użytkownikom wewnątrz ich sesji.
- Rozdział 8, „Zabezpieczanie połączeń RDP”, omawia szyfrowanie RDP, uwierzytelnianie serwera i klienta oraz konfigurowanie ustawień zabezpieczeń na serwerze RD Session Host.
- Rozdział 9, „Wdrożenia wieloserwerowe”, wprowadza kluczowe koncepcje wieloserwerowych rozwiązań, pokazuje budowanie farm serwerów RD Session Host i wyjaśnia, jak publikować aplikacje i prezentować zasoby poprzez RD Web Access.
- Rozdział 10, „Zapewnianie dostępności RDS z Internetu”, ukazuje, jak zainstalować i skonfigurować usługę roli RD Gateway w celu zapewnienia dostępu do programów RemoteApps, sesji pulpitu oraz maszyn wirtualnych użytkownikom zlokalizowanym poza siecią firmy.
- Rozdział 11, „Zarządzanie sesjami pulpitu zdalnego”, ukazuje, jak monitorować i kończyć procesy i sesje użytkowników uruchomione na serwerze RD Session Host, jak zapewnić pomoc przy użyciu zdalnego sterowania i jak opróżnić serwer w razie konieczności jego konserwacji.
- Rozdział 12, „Licencjonowanie usług pulpitu zdalnego”, przedstawia nowe zasady licencjonowania RDS: zarówno licencjonowanie usług pulpitu zdalnego, jak i infrastruktury wirtualnych pulpitów. Rozdział ten wyjaśnia też, jak licencje są śledzone lub wymuszane; jak serwer RD License przydziela licencje RDS CAL; jak zainstalować, skonfigurować i utrzymywać serwery licencji; jak diagnozować problemy dotyczące licencjonowania i jak migrować licencje z jednego serwera na drugi.

Konwencje stosowane w tej książce

Poniższa książka zawiera następujące elementy służące wyróżnieniu szczególnie istotnych informacji.

Uwagi dla Czytelnika

Poniższe uwagi w ramkach mają na celu zwrócenie uwagi na istotne informacje.

Rodzaj ramki	Znaczenie
Ostrzeżenie	Przestrzega, że pominięcie lub podjęcie określonego działania może spowodować poważne problemy dla użytkowników, systemu, integralności danych i tak dalej.
Uwaga	Podkreśla znaczenie specyficznej koncepcji lub zwraca uwagę na szczególne przypadki, które mogą nie mieć zastosowania w każdej sytuacji.
Na dołączonym nośniku	Zwraca uwagę na związany z bieżącym tematem skrypt, program, szablon lub łącze URL znajdujące się na dołączonym do książki dysku CD.

Ramki

Szersze fragmenty umieszczone w ramkach zawierają dodatkowe informacje, wskazówki lub porady dotyczące różnych funkcji Remote Desktop Services.

Ramka	Znaczenie
Wprost ze źródła	Wskazówki i uwagi napisane przez ekspertów z grupy projektowej produktu, udostępniające wgląd w budowę i działanie Remote Desktop Services, a także zalecenia i wskazówki rozwiązywania problemów.
Z praktyki	Rzeczywiste doświadczenia ekspertów zewnętrznych w stosunku do grupy projektowej produktu. Niektórzy autorzy to inżynierowie zatrudnieni w firmie Microsoft; inni to Microsoft MVP lub inni specjaliści.
Jak to działa	Zapewnia unikalne wejrzenie w funkcjonowanie Remote Desktop Services i elementów tej roli.

Przykłady poleceń trybu znakowego

Poniższe konwencje są używane przy dokumentowaniu przykładów poleceń.

Styl	Znaczenie
Czcionka wytłuszczona	Wskazuje tekst wpisywany przez użytkownika (znaki wpisywane dokładnie tak, jak pokazano).
Kursywa	Oznacza zmienne, którym należy nadać właściwą wartość (na przykład *filename* należy zastąpić faktyczną nazwą pliku).
`Czcionka stałopozycyjna`	Używana w przykładach kodu oraz wynikach działania narzędzi wiersza polecenia.
%VariableName%	Zmienne środowiskowe.

Uwagi dotyczące polskiej wersji

System Windows Server 2008 R2 dostępny jest w polskiej wersji interfejsu, jednak w odróżnieniu do systemów klienckich, stosunkowo niewielka część zainstalowanych serwerów wykorzystuje tę wersję. Dodatkowo część narzędzi systemowych, nazwy kluczy rejestru i wiele innych odwołuje się do angielskich nazw programów, usług czy funkcji. Z tego względu książka posługuje się zasadniczo terminologią pochodzącą z wersji angielskiej. Przy pierwszym użyciu jakiegoś terminu jest on uzupełniany polską wersją umieszczoną w nawiasie.

Większość komponentów roli *Remote Desktop Services* ma długie, wielowyrazowe nazwy, które w wersji polskiej stają się jeszcze dłuższe. Ze względu na czytelność w całej książce powszechnie stosowane są akronimy pochodzące od angielskich nazw tych komponentów. Najczęściej używane akronimy (także dotyczące innych elementów systemu) zostały zebrane w tabeli.

Skrót	Termin angielski	Termin polski
AD DS	Active Directory Domain Services	Usługi domenowe w usłudze Active Directory
API	Application Programming Interface	Interfejs programowania aplikacji
DVC	Dynamic Virtual Channel	Dynamiczny kanał wirtualny
GPMC	Group Policy Management Console	Konsola zarządzania zasadami grupy
GPO	Group Policy Object	Obiekt zasad grupy
IE	Internet Explorer	
IIS	Internet Information Services	Internetowe usługi informacyjne
MVP	Most Valuable Professional	– (*termin nie jest tłumaczony*)
NLB	Network Load Balancing	Równoważenie obciążenia sieciowego
OU	Organizational Unit	Jednostka organizacyjna
PDU	Protocol Data Unit	Jednostka danych protokołu
RD	Remote Desktop	Pulpit zdalny
RDC	Remote Desktop Connection	Podłączanie pulpitu zdalnego (RDC)
RDCB	RD Connection Broker	Broker sesji połączenia pulpitu zdalnego
RDP	Remote Desktop Protocol	– (*termin nie jest tłumaczony*)
RDS	Remote Desktop Services	Usługi pulpitu zdalnego
RDSH	Remote Desktop Session Host	Host sesji usług pulpitu zdalnego
RDVH	Remote Desktop Virtualization Host	Host wirtualizacji pulpitu zdalnego
UMDF	UserMode Driver Framework	Struktura sterowników trybu użytkownika
URL	Uniform Resource Locator	– (*termin nie jest tłumaczony*)
VD	Virtual Device	urządzenie wirtualne
VDI	Virtual Desktops Infrastructure	Infrastruktura pulpitów wirtualnych
VM	Virtual Machine	maszyna wirtualna
VP	Virtual Processor	procesor wirtualny
WMI	Windows Management Instrumentation	Instrumentacja zarządzania systemu Windows

Korzystanie z obrazu dysku CD

Obraz dysku CD towarzyszącego książce jest dostępny na stronie wydawcy przy opisie książki w zakładce Dodatkowe informacje, pod adresem:

http://www.ksiazki.promise.pl/aspx/produkt.aspx?pid=57882

Na podstawie tego obrazu można wykonać fizyczny dysk CD lub zainstalować go jako napęd wirtualny. Wymagania sprzętowe dla korzystania z tego dysku znajdują się na końcu książki. Dysk ten zawiera następujące zasoby:

- **Łącza** Dysk zawiera wiele łączy do adresów URL, zapewniających dostęp do dodatkowych informacji, narzędzi, skryptów i innych źródeł, takich jak strony partnerskie.

- **Skrypty** Znajdziemy tu kolekcję skryptów ilustrujących sposoby pracy z RDS przy użyciu Windows PowerShell oraz VBScript. W odpowiednich miejscach książki zamieszczono ich wydruki, dzięki czemu można łatwiej zrozumieć, jak te skrypty zapewniają funkcjonalność, której potrzebujemy. Choć skrypty te są pomyślane jako przykłady, a nie gotowe produkty, zapewniają dostęp do takich informacji, które nie są osiągalne w GUI i można łatwo dostosować je do własnych potrzeb.

Dodatkowe treści online W miarę jak nowe lub zaktualizowane materiały uzupełniające tę książkę staną się dostępne, będą one umieszczane online. Mogą to być erraty, aktualizacje, łącza do dodatkowych materiałów i tak dalej. Witryna ta jest dostępna pod następującym adresem *http://go.microsoft.com/fwlink/?LinkId=203980* i jest regularnie aktualizowana.

ROZDZIAŁ 1

Wprowadzenie do RDS

Może być wiele powodów, dla których Czytelnik mógł sięgnąć po tę książkę. Być może od dawna korzysta z Microsoft Terminal Server i chciałby się dowiedzieć, co Usługi pulpitu zdalnego (Remote Desktop Services – RDS[1]) w systemie Windows Server 2008 R2 mogą mu dać. Albo właśnie zainstalował Windows Server 2008 R2 i jest zainteresowany tym, jak działają te wszystkie role i funkcje dostępu przez sieć Web, bramy czy host usług dostępu zdalnego. Wreszcie ktoś mógł słyszeć coś o RDS i chciałby skorzystać z włączenia tego rozwiązania w swoim środowisku. W każdym przypadku zapewne pojawi się pytanie, na czym polegają podobieństwa i różnice pomiędzy RDS a innymi technikami dostępu zdalnego w systemie Windows Server 2008 R2.

Bez względu na to, jaka jest przyczyna zainteresowania rozwiązaniami RDS, książka ta zawiera potrzebne informacje.

Rozdział ten ma na celu zbudowanie podstawy dla całej reszty książki. Aby móc zrozumieć ewolucję Microsoft Terminal Services (obecnie nazywanych Usługami pulpitu zdalnego), Czytelnik musi zrozumieć, skąd się one wzięły i poznać „ekosystem", w którym funkcjonują. Aby zrozumieć, co możemy zrobić przy użyciu tych wszystkich ról i usług, musimy poznać podstawowe cele, dla których utworzono RDS, oraz scenariusze, w których można je wykorzystać. A ponieważ RDS nie jest bytem samoistnym, ale fragmentem szerszej infrastruktury, pokażemy, jak mechanizm ten współdziała z innymi rozwiązaniami, takimi jak Hyper-V lub IIS.

1 Dla zachowania przejrzystości odwołuję się do terminologii anglojęzycznej, czyli występującej w angielskiej wersji systemu operacyjnego. Przy pierwszym użyciu nazwy roli, usługi lub funkcji dołączana jest polska nazwa zawarta w nawiasach. Polskich określeń używam tam, gdzie są one traktowane jako rzeczowniki pospolite (a nie nazwy własne). Stąd pulpit zdalny jako ogólne pojęcie, ale Remote Desktop Services (albo RDS) jako nazwa określonego rozwiązania technicznego.

Po przeczytaniu tego rozdziału Czytelnik będzie wiedział:

- Dlaczego Terminal Services nazywają się obecnie Remote Desktop Services.
- Jakie składniki Windows Server 2008 R2 wspierają środowisko RDS.
- Jakie scenariusze wspierają poszczególne usługi roli RDS.
- Jakie rodzaje nowych technologii udostępniają te scenariusze.
- Jak poszczególne usługi roli RDS oddziałują ze sobą nawzajem.
- Jak usługi roli RDS są zależne od innych ról Windows Server.
- Jakie interfejsy programowania aplikacji (API) są dostępne dla projektantów i programistów oraz przykłady funkcji, które programiści mogą dołączyć do RDS.

Skąd wziął się RDS?

Komuś, kto po raz pierwszy spotkał się z RDS w Windows Server 2008 R2, trudno będzie rozpoznać jego wcześniejsze wcielenia. Podobnie jak sam Windows Server, RDS uległ *znaczącym* przemianom w ciągu minionych lat i stał się znacznie bardziej wszechstronny. Nie jest konieczne przeglądanie wyczerpującej listy funkcji każdej kolejnej edycji, ale warto przyjrzeć się temu, jak koncepcja wielodostępu w Windows rozwijała się od swego powstania w połowie lat dziewięćdziesiątych minionego stulecia.

Citrix MultiWin

Oryginalna architektura MultiWin nie została zaprojektowana przez Microsoft, ale przez firmę Citrix, która nabyła licencję na kod źródłowy Windows NT 3.51 w celu stworzenia wielodostępnego systemu Windows[2]. Citrix stworzył swój własny produkt o nazwie WinFrame, będący wieloużytkownikową wersją Windows NT 3.51, jednak całkowicie odseparowany od systemu operacyjnego tworzonego i oferowanego przez Microsoft.

Windows NT, Terminal Server Edition

WinFrame został zbudowany na bazie Windows NT 3.51. W 1995 roku Microsoft odkupił licencję MultiWin od Citrixa i wmontował wieloużytkownikowe jądro w podstawową wersję Windows NT 4.0, aby stworzyć nowy produkt: Windows Server z możliwością pracy wieloużytkownikowej. Wynikiem tych działań był Windows NT 4.0 Terminal Server Edition. Citrix nie oferował już samodzielnego produktu, ale opublikował MetaFrame, działający w Terminal Server Edition (bardzo podobnie do tego, jak dziś Citrix XenApp działa w Windows Server) i dodający kilka nowych funkcji i narzędzi administracyjnych.

Terminal Server Edition był w istocie tylko początkiem. System operacyjny był bardzo podstawowy, łagodnie ujmując. Niemal każda instalacja Terminal Server Edition wykorzystywała dodatkowo MetaFrame, gdyż sam podstawowy produkt nie zapewniał praktycznie nic poza udostępnianiem samego systemu wieloużytkownikowego. Nie zawierał nawet

2 MultiWin oryginalnie miał być oparty na IBM Operating System/2 (OS/2), gdy Microsoft stanowił jeszcze część projektu OS/2, ale ostatecznie system Windows zwyciężył.

Pierwsze doświadczenia z wieloużytkownikowymi Windows

Christa pierwszy raz miała do czynienia z wieloużytkownikowym środowiskiem Windows w postaci WinFrame 1.7 w 1997 roku w centrum szkoleniowym IBM w Hudson River Valley w stanie Nowy Jork. Szkolenie trwało wiele dni, toteż centrum to dysponowało własnymi pokojami hotelowymi. Początkowo centrum to udostępniało komputer PC w każdym pokoju gościnnym i personel musiał poradzić sobie z koszmarem zarządzania każdym z nich. Jednak od owej sesji szkoleniowej w 1997 rozpoczęli konfigurowanie stacji typu *thin client* (podłączonych do serwerów WinFrame) we wszystkich pokojach dla gości, aby dać im dostęp do poczty i możliwość pracy w swoich pokojach. Gdy uczestnik szkolenia się rejestrował, skrypt automatycznie tworzył dla niego konto użytkownika. Dziś nie ma w tym niczego nadzwyczajnego, ale wówczas było to bardzo mocne rozwiązanie i ogromna zmiana w stosunku do tradycyjnego, zorientowanego na indywidualną maszynę, modelu systemu Windows.

tak elementarnej funkcjonalności, jak mapowanie schowka. Także fakt, że Terminal Server Edition i zasadniczy system operacyjny były różnymi produktami, nie stanowił zalety ani z punktu widzenia firmy Microsoft, ani jej klientów. Microsoft musiał radzić sobie z obsługą dwóch zestawów pakietów serwisowych i poprawek, zaś klienci musieli kupić oddzielny produkt, aby wypróbować przetwarzanie oparte o serwer *oraz* żonglować dwoma różnymi pakietami serwisowymi, które dodatkowo nie były publikowane w tym samym czasie. Na plus można tylko dodać, że gdy ujawnił się poważny problem z Service Pack 6 (SP6) dla Windows NT 4.0, został on już rozwiązany, gdy przyszła pora na publikację SP6 dla Terminal Server Edition.

Windows 2000 Server

Pierwszym prawdziwym przełomem w rozwoju środowisk wieloużytkownikowych był Microsoft Windows 2000 Server. Po raz pierwszy Terminal Services (czyli usługi terminalowe) stały się rolą serwera podstawowej edycji systemu operacyjnego, a nie oddzielnym produktem. Dlaczego to jest ważne? Można wymienić kilka powodów. Po pierwsze, zakończyły się problemy ze wzajemnie niekompatybilnymi pakietami serwisowymi dla wersji jedno- i wieloużytkownikowych. Po drugie, nastąpiła fundamentalna zmiana w sposobie postrzegania przetwarzania opartego na serwerze i dostępu zdalnego. Przed wydaniem Windows 2000, jeśli ktoś chciał zarządzać serwerem Windows za pośrednictwem środowiska graficznego (GUI), zasadniczo musiał użyć jego lokalnej konsoli (klawiatury i monitora) – nie było możliwości zdalnego zarządzania, jakie daje pulpit zdalny, czyli Remote Desktop Protocol (RDP). Problem w tym, że liczba serwerów, przy których można zasiąść w ciągu dnia, jest ograniczona – zwłaszcza wtedy, gdy serwery te stoją w różnych budynkach, a nawet w różnych miastach. Wydanie Windows 2000 Server wprowadziło Remote Administration jako komponent opcjonalny, pozwalając administratorom serwerów na zarządzanie systemami *bez* konieczności spacerów do serwerowni. Nie tylko znacząco uprościło to pracę

administratorów, ale zarazem rozpropagowało ideę Terminal Services, gdyż dało ludziom dobry i codzienny przykład pracy zdalnej i przetwarzania wieloużytkownikowego.

Dostępność Terminal Services w trybie serwera aplikacji w podstawowym systemie operacyjnym oznaczało również, że próba udostępnienia serwera terminali użytkownikom wymagała stosunkowo niewielkiego wysiłku – skonfigurowanie pilotażowej instalacji można było wykonać po prostu instalując rolę w trybie serwera aplikacji i pozwalając użytkownikom skorzystać choćby z Notatnika. Ponadto, ponieważ RDP w Windows 2000 Server dodał pewne podstawowe funkcjonalności, jak przekierowanie drukarki klienckiej czy współużytkowany schowek dla sesji lokalnej i zdalnej, testowanie serwera terminali i sprawdzenie, czy i jak użytkownicy mogliby skorzystać z współdzielonego przetwarzania, było możliwe przy użyciu samych tylko narzędzi wchodzących w skład systemu operacyjnego.

Windows Server 2003

Kolejnym wielkim krokiem był Microsoft Windows Server 2003, w którym niektóre decyzje podjęte przy projektowaniu Windows 2000 Server zostały rozwinięte zgodnie z ich logicznymi konsekwencjami. Jeśli Remote Administration było rzeczą dobrą, dlaczego miałby to być składnik opcjonalny? Zamiast tego, włączono ten mechanizm dla wszystkich roli serwera i uczyniono go opcją systemów klienckich. A chociaż podstawowa funkcjonalność Windows 2000 Terminal Server była użyteczna, nie udostępniała dostatecznie bogatego środowiska klienckiego. Zatem włączmy mapowanie dysków, pełny kolor, dźwięk i inne funkcje, które dotąd były osiągalne tylko przy użyciu dodatkowych produktów innych firm, aby wrażenia przy pracy zdalnej były możliwie zbliżone do pracy na lokalnym systemie.

Inna wielka zmiana, która nastąpiła w Windows Server 2003, dotyczyła zarządzania. Serwery terminali Windows 2000 mogły być zarządzane tylko pojedynczo. Można było konfigurować je zdalnie, ale nie zbiorczo. Windows Server 2003 wprowadził kilka ustawień zasad grupy, które pozwalają na konfigurowanie i zarządzanie serwerami terminali, zaś narzędzie Terminal Server Manager wspierało administrowanie zdalnymi serwerami.

Windows Server 2008

Microsoft Windows Server 2008 stanowi wielki skok w funkcjonalności usług terminalowych. Wcześniejsze wersje zawierały tylko dwie role: serwera terminali i serwera licencji.

> **Wskazówka** Choć Windows Server 2003 zawierał komponent Session Directory Server, zapewniający podstawowe wsparcie dla farm serwerów, rola ta była dostępna tylko w wydaniu Enterprise i nie została szeroko rozpowszechniona.

Jeśli potrzeby wykraczały poza zdalny dostęp do pełnych funkcji pulpitu w sieci lokalnej, konieczne było wykorzystanie dodatków innych firm, aby spełnić oczekiwania. Wraz z opublikowaniem Windows Server 2008, Terminal Services uzyskały następujące możliwości dodatkowe:

- Wizualną integrację pomiędzy aplikacjami uruchamianymi lokalnie i zdalnie.

- Interfejs oparty o Web, umożliwiający indywidualne prezentowanie aplikacji dostępnych na serwerze terminali.
- Bezpieczną bramę, zapewniającą zabezpieczony dostęp przez Internet.
- Brokera sesji, kierującego przychodzące połączenia do najbardziej odpowiedniego serwera terminali.
- Podsystem drukowania, który nie wymagał instalowania sterowników drukarek na serwerach terminali.
- Przekierowanie nowych typów urządzeń.

Windows Server 2008 R2 i RDS

Technicznie ujmując, Windows Server 2008 R2 to „pomniejsza" aktualizacja, podobnie jak inne wersje R2, jednak wprowadza wiele zmian w funkcjonalności RDS. Usługi roli zostały ponownie rozszerzone w celu dodania wsparcia dla wirtualnego pulpitu (często nazywanego VDI od *Virtual Desktop Infrastructure*). Pojawiły się też nowe funkcje, z których najbardziej istotne są następujące:

- Wsparcie dla połączeń do pul współużytkowanych maszyn wirtualnych (VM) opartych na Hyper-V i przypisywanie osobistych maszyn wirtualnych poszczególnym osobom.
- Zmiany w mechanizmie Remote Desktop Web Access, pozwalające portalowi na wyświetlanie zasobów z wielu serwerów Remote Desktop Session Host[3] (Host sesji pulpitu zdalnego), wcześniej nazywanych serwerami terminali, i pozwalające na filtrowanie programów RemoteApp i maszyn wirtualnych na podstawie ustawień zabezpieczeń.
- Ulepszona zgodność aplikacji i zarządzanie zasobami na RDSH.
- Wsparcie dla zdalnego dostępu do środowiska Aero i inne ulepszenia w wersji RDP 7.
- Wsparcie dla mechanizmu pojedynczego logowania (*single sign-on*) opartego na formularzach poprzez RD Web Access, dzięki czemu użytkownicy muszą tylko raz uwierzytelnić się w witrynie, aby uzyskać dostęp do wszystkich przypisanych im aplikacji RemoteApp.
- Usprawnienia mechanizmu Remote Desktop Gateway, umożliwiające wymuszenie przekierowania napędów i włączenie trybu naprawy klienta dla tych systemów, które nie są zgodne z ustalonymi zasadami.
- Ulepszone wykrywanie serwerów licencji w celu podniesienia niezawodności połączeń.

Najbardziej oczywistą, choć najmniej istotną zmianą, jest fakt, że Terminal Services nazywają się teraz Remote Desktop Services (Usługi pulpitu zdalnego) i wszystkie podrzędne role zostały również odpowiednio przemianowane. Zmiana nazwy usługi ma na celu lepsze odzwierciedlenie znacznie szerszego zakresu tej roli serwera, nie ograniczającej się tylko do udostępniania sesji i usług roli koniecznych do zapewnienia łączności, ale także utrzymywanie maszyn wirtualnych i bezpiecznego dostępu z sieci rozległej (WAN).

3 Dla zachowania czytelności w książce stosowany jest akronim RDSH, pochodny od angielskiej nazwy tej usługi roli.

Wprost ze źródła

Dlaczego VDI?

Michael Kleef, Senior Product Manager
Windows Server Marketing

Microsoft dołączył wsparcie dla VDI w wersji Windows Server 2008 R2, aby umożliwić klientom większe możliwości udostępniania zasobów w trybie pracy *thin client*. Choć RDSH jest w pełni rozwiniętym produktem i zapewnia klientom dobry wskaźnik TCO (*Total cost of Ownership* – całkowity koszt posiadania), istnieją sytuacje, w których poziom personalizacji i izolacji zapewniany przez VDI jest ważny. Aplikacje wymagające podniesionych uprawnień trudno obsługiwać w normalnym trybie RDSH, gdyż jeden błąd popełniony przy podniesionych uprawnieniach może wpłynąć na wszystkich użytkowników serwera. Izolacja maszyn wirtualnych umożliwia wsparcie dla tego typu aplikacji. Innym przykładem może być własna kompatybilność aplikacji. Problem ten w znacznym stopniu rozwiązuje mechanizm Microsoft App-V, ale nie radzi on sobie ze wszystkimi problemami, gdy aplikacja wymaga instalacji klienta Windows. Z takich powodów Microsoft zainwestował w stworzenie platformy VDI w systemie Windows Server 2008 R2 i rozszerzył ją dalej w Service Pack 1 o mechanizmy Dynamic Memory oraz RemoteFX, aby zwiększyć gęstość uruchamianych maszyn wirtualnych i poprawić wrażenia użytkowników.

Uwaga Ponieważ książka ta dotyczy Windows Server 2008 R2, wykorzystuje bieżące nazwy ról serwera i usług roli. Tabela 1-1 zawiera listę nazw, które pojawiać się będą najczęściej. Pełne mapowanie starych i nowych nazw dotyczących RDS zawiera artykuł *http://technet.microsoft.com/en-us/library/dd560658(WS.10).aspx*.

Tabela 1-1 Mapowanie nazw Terminal Services na nazwy RDS

Dawna nazwa	W wersji polskiej	Nazwa w Windows Server 2008 R2	W wersji polskiej
Terminal Services (TS)	Usługi terminalowe	Remote Desktop Services (RDS)	Usługi pulpitu zdalnego
Terminal Server	Serwer terminali	Remote Desktop Session Host (RDSH)	Host sesji usług pulpitu zdalnego
TS Licensing	Licencjonowanie usług terminalowych	Remote Desktop Licensing (RD Licensing)	Licencjonowanie usług pulpitu zdalnego
TS Web Access	Dostęp w sieci Web do usług terminalowych	RD Web Access	Dostęp w sieci Web do usług pulpitu zdalnego
TS Gateway	Brama usług terminalowych	RD Gateway	Brama usług pulpitu zdalnego

Tabela 1-1 Mapowanie nazw Terminal Services na nazwy RDS

Dawna nazwa	W wersji polskiej	Nazwa w Windows Server 2008 R2	W wersji polskiej
Terminal Services Client Access License (TS CAL)		Remote Desktop Services Client Access License (RDS CAL)	
Terminal Services Manager	Menedżer usług terminalowych	Remote Desktop Services Manager	Menedżer usług pulpitu zdalnego
Terminal Services Configuration	Konfiguracja usług terminalowych	Remote Desktop Services Configuration	Konfiguracja usług pulpitu zdalnego

Jak widać, wzorzec jest dość prosty. Jeśli więc zauważymy nazwę funkcji lub usługi, która wydaje się niezrozumiała, warto sprawdzić powyższą listę i poszukać analogii.

Ewolucja funkcjonalności klienta dostępu zdalnego

Choć książka ta koncentruje się przede wszystkim na zagadnieniach współużytkowania komputera (serwera), a nie na oprogramowaniu klienckim, ważne jest, abyśmy wiedzieli, że zmiany dotyczące RDS dotyczą również możliwości dostępnych po stronie klienckiej. Systemy klienckie Windows aż do wersji Windows 2000 Professional nie zapewniały wsparcia dla przychodzących połączeń pulpitu zdalnego (inaczej mówiąc, systemy te nie mogły pełnić funkcji serwera terminali), ale począwszy od Windows XP funkcja ta jest dostępna we wszystkich wersjach. Wsparcie dla przychodzących połączeń sprawiło, że możliwe stały się nowe sposoby wykorzystania klienckich systemów, w tym:

- Zdalny dostęp do fizycznego komputera z innego miejsca, np. z domu lub innego biura.
- Remote Assistance (Pomoc zdalną).
- Hosting pulpitów wirtualnych.
- Hosting programów RemoteApp, które są dostępne w innym klienckim systemie operacyjnym (w celu zapewnienia funkcjonowania programów niekompatybilnych z bieżącym systemem).

Dostęp zdalny z innego komputera jest odpowiedzią na coraz powszechniejszy fakt, że wiele osób używa więcej niż jednego komputera, a także że nawet domowe środowisko może zawierać kilka komputerów. Mechanizm Pomocy zdalnej wykorzystuje funkcje zdalnego sterowania RDS – możliwość zezwolenia innej osobie na oglądanie, a nawet na przejęcie sesji zdalnej – do usprawnienia działania pracowników pomocy technicznej. Hosting pulpitów wirtualnych przez długi czas był jednym z głównych konkurentów dla koncepcji hostowania sesji (i obecnie stał się częścią tej usługi). Funkcje takie jak RemoteApp oparte na Hyper-V umożliwiają uruchamianie aplikacji wymagających starszego systemu operacyjnego i dostępu do nich z nowszego, nawet jeśli aplikacja taka z jakiegoś powodu nie może działać bezpośrednio w Windows 7.

Uwaga Mówiąc najogólniej, większość 32-bitowych aplikacji powinna działać na platformie 64-bitowej, pod warunkiem, że nie zawierają sterowników urządzeń i nie wykorzystują 16-bitowych procedur instalacyjnych. Aplikacje Web zaprojektowane do uruchamiania w przeglądarce Internet Explorer 6 stanowią wyjątek od tej reguły. IE 6 jest częścią Windows Server 2003, ale nie można go zainstalować w systemie Windows Server 2008 R2. Tym samym, aby aplikację zależną od dostępności Internet Explorer 6 móc wyświetlić jako program RemoteApp, należy ulokować ją w maszynie wirtualnej przy użyciu RemoteApp for Hyper-V.

RDS pojawia się w klienckich wersjach Windows nawet wtedy, gdy tego nie oczekujemy. To właśnie ta technika umożliwia szybkie przełączanie użytkowników i pomoc zdalną (aby wymienić tylko dwie), zaś od wersji protokołu RDP zależy dostępność rozwiązania Live Mesh.

Mówiąc w skrócie, opowieść o usługach pulpitu zdalnego to historia tego, jak wielоużytkownikowe przetwarzanie stało się mniej niszową technologią, a bardziej strategią udostępniania najrozmaitszych rozwiązań, które zacierają granicę pomiędzy komputerem osobistym a serwerownią. Nawet jeśli niektóre z nich nie zawierają „RDS" w nazwie, wielоużytkownikowe przetwarzanie i Remote Desktop Protocol (RDP) stały się krytycznymi częściami podstawowej platformy Windows.

Co możemy zrobić przy użyciu RDS?

W poprzednim podrozdziale przedstawiliśmy (bardzo krótki) przegląd historii RDS i jak stały się one częścią jądra platformy Windows – zarówno po stronie klienta, jak i serwera. Pogłębione omówienie tej technologii zawarte jest w kolejnych rozdziałach książki. Spróbujmy jednak postawić pytanie, co możemy *zrobić* przy ich użyciu?

Zasadniczo, zdalny pulpit łamie sztywne powiązania pomiędzy lokalizacjami, systemami klienckimi i dostępnymi możliwościami.

Pod wieloma względami jest to naturalne rozszerzenie koncepcji pracy sieciowej. Jeśli używamy pojedynczego komputera, który nie jest podłączony do żadnej sieci, jesteśmy ograniczeni do aplikacji i danych przechowywanych na tym komputerze. Jeśli dołączymy ten komputer do sieci i uaktywnimy udostępnianie plików, możemy korzystać z danych, które nie są przechowywane na nim, a administrator systemu może zająć się zarówno tworzeniem kopii zapasowych tych danych (co byłoby niewykonalne w przypadku izolowanego komputera), jak i ich zabezpieczeniami. Przy wykorzystaniu RDS można nie tylko korzystać z danych zlokalizowanych gdzieś indziej, ale również z umieszczonych tam programów. Co więcej, aplikacje te nie muszą nawet spełniać wymogu możliwości uruchamiania na komputerze klienckim, o ile mogą być uruchamiane na hoście. „Uzdalnienie" prezentacji usprawnia udostępnianie plików, gdyż pliki, z których korzystamy, nie muszą być nawet dostępne dla samego komputera klienckiego, o ile tylko są one dostępne dla hosta, na którym uruchamiana jest aplikacja.

W przypadku izolowanego komputera jesteśmy całkowicie przywiązani do tego, co ten komputer jest w stanie zrobić. W przypadku uzdalniania prezentacji możliwości stają się szersze, gdyż to, co widzimy, niekoniecznie jest wykonywane przez używany przez nas

komputer – rzeczywisty wykonawca może znajdować się gdzie indziej, nawet w innym kraju. Daje to niezrównane korzyści pod względem niezależności od sprzętu i lokalizacji oraz poziomu zabezpieczeń.

Zwiększone zabezpieczenia użytkowników zdalnych

Przetwarzanie danych całkowicie oparte na komputerze osobistym tworzy problemy dotyczące bezpieczeństwa danych. Coraz większa liczba użytkowników wykorzystuje komputery przenośne, zaś te – jak sama nazwa wskazuje – są zabierane w najrozmaitsze miejsca. Jednak laptop zawierający dane pociąga za sobą zagrożenie dla bezpieczeństwa, nawet jeśli zostanie jakoś zabezpieczony hasłem czy szyfrowaniem. Jeśli nie będziemy go ze sobą nosić *wszędzie*, nawet wybierając się na kolację (zamiast zostawić go w pokoju hotelowym), dane w nim zawarte mogą stać się celem kradzieży. A jeśli ktoś *naprawdę* zechce zdobyć nasz laptop, nie ma znaczenia, jak dobrze będziemy go pilnować – nie wspominając o tak częstych przypadkach, jak pozostawienie komputera w taksówce czy pociągu. To się po prostu zdarza. Rozwiązania BitLocker wprowadzone w Windows Vista i Windows 7 pozwalają uchronić się przed kradzieżą danych, ale nie chronią nas samych przed *utratą* danych, które znajdowały się na skradzionym lub zniszczonym laptopie i nigdy nie utworzono ich kopii zapasowej.

Jeśli komputer zawiera dane i stracimy go z jakiegokolwiek powodu, dane te również są stracone. Oczywistym i najprostszym rozwiązaniem jest nieprzechowywanie danych na tym komputerze – zapisujmy je w firmowym centrum przetwarzania danych. Jednak jeśli łączymy się z tym centrum ze zdalnej lokalizacji poprzez wirtualną sieć prywatną (VPN) i pracujemy nad dużymi plikami (jakie pliki *nie są* duże w dzisiejszych czasach?), pojawia się pokusa zapisania pliku na dysku lokalnym podczas pracy zdalnej i skopiowania go z powrotem po zakończeniu pracy. Jeśli jednak będziemy pracować w ten sposób, znajdziemy się ponownie w punkcie wyjścia – z danymi (być może poufnymi), zapisanymi na lokalnym dysku komputera.

Jednym z rozwiązań dylematu, jak zabezpieczyć dane, zarazem zapewniając ich dostępność dla tych użytkowników, którzy ich potrzebują, jest przechowywanie *wszystkiego* w centrum danych, łącznie z aplikacjami wymaganymi do edycji. Jeśli zarówno dane, jak i aplikacje są zlokalizowane w sieci, niemożliwe staje się lokalne edytowanie danych (gdyż żadna aplikacja, która to umożliwia, nie jest zainstalowana na lokalnych komputerach), ale też nie występuje taka potrzeba, gdyż nie ma żadnego powodu pobierania zdalnego pliku do komputera lokalnego w celu (na przykład) podniesienia wydajności. Żadne poufne dane nie są zapisywane na komputerze lokalnym. Cały czas wszystko pozostaje wewnątrz bezpiecznych ścian serwerowni.

Co jednak, jeśli chcielibyśmy, aby użytkownicy mogli edytować poufne dokumenty, gdy znajdują się w bezpiecznej lokalizacji, ale nie wówczas, gdy łączą się z siecią korporacyjną z kafejki internetowej? Jeśli korzystamy z RDS w Windows Server 2008 R2, możemy skonfigurować reguły, które określą, do jakich aplikacji zdalny użytkownik będzie miał dostęp, czy może zamapować lokalne dyski i czy możliwe będzie wycinanie i wklejanie tekstu lub innych danych pomiędzy aplikacjami lokalnymi i zdalnymi. Potrzeby zabezpieczeń mogą określić ograniczenia nakładane na dostęp zdalny, jednocześnie zapewniając łatwy dostęp do danych tam, gdzie powinny być one osiągalne.

(Nie)bezpieczeństwo informacyjne

Ograniczanie dostępu do poufnych informacji tylko dla osób znajdujących się w czterech ścianach biura nie jest praktyczne, ale ciągle pojawiają się przykłady, co może się stać, gdy informacje takie opuszczą centrum przetwarzania danych. W listopadzie 2009 wojskowy korpus inżynieryjny stracił dysk twardy zawierający nazwiska i numery ubezpieczenia społecznego blisko 60 tysięcy bieżących i byłych pracowników – zarówno wojskowych, jak i cywilnych. W momencie pisania tych słów dysk ten nie został jeszcze odzyskany. Nie jest to pierwszy przypadek, gdy poufne dane zostały utracone z powodu kradzieży bądź zagubienia laptopa lub innego przenośnego medium.

Nie zawsze realne jest przechowywanie poufnych danych tylko w zabezpieczonej serwerowni, dostępnych tylko za pośrednictwem bezpiecznych łączy do hosta sesji pulpitu zdalnego, zlokalizowanego poza siecią osłonową. Niekiedy informacje muszą być dostępne także wtedy, gdy nie ma możliwości utworzenia łącza sieciowego. Jednak jeśli to jest wykonywalne, znacznie bezpieczniej jest przechowywać dane tam, gdzie będą mniej narażone na ujawnienie, kradzież lub utratę: w centrum przetwarzania danych.

Uwaga Przy wystarczająco dużej odległości lub dostatecznie powolnym łączu internetowym, połączenie pulpitu zdalnego również będzie działało powoli. Jeśli zaś łącze sieciowe nie jest wystarczająco niezawodne, może powodować frustrację z powodu powtarzających się przerw i rozłączeń. Wiemy aż za dobrze, że nawet sieci wielkiej prędkości wykazują pewne opóźnienia, gdy pracujemy na jednym kontynencie, a centrum danych znajduje się na innym. Jednak problemy te dotyczą każdego scenariusza dostępu zdalnego i stwarzają mniejsze ryzyko przypadkowego uszkodzenia oryginalnego dokumentu niż próba nadpisania go lokalnie przeedytowaną kopią przez powolne łącze. Zerwana sesja nie powoduje utraty danych – ona po prostu czeka na ponowne połączenie użytkownika.

Szybkie wyposażanie nowych użytkowników

Ta opcja jest szczególnie przydatna w przypadku pracowników tymczasowych. Jeśli musimy udostępnić usługi informatyczne komuś, kto będzie tu pracował tylko chwilowo (na przykład konsultant wymagający dostępu do systemu na czas wykonywanej pracy), dobrze byłoby nie musieć poświęcać zbyt wiele czasu na konfigurowanie dla niego komputera, ale równie dobre będzie danie mu czystego środowiska, bez konieczności radzenia sobie z najrozmaitszymi „pozostałościami” po poprzednim użytkowniku. Dzięki RDS nowy użytkownik może rozpocząć pracę natychmiast po przypisaniu mu konta domenowego. Dodatkowo pula maszyn wirtualnych lub sesja zdalnego pulpitu wykorzystywana przez tę osobę będzie całkowicie nowa, bez żadnych ustawień nadanych przez wcześniejszych użytkowników, co powinno uprościć rozwiązywanie problemów i szkolenie.

Umożliwianie pracy zdalnej

Zagadnieniem związanym z bezpieczeństwem dla pracowników mobilnych jest praca zdalna. Telepraca staje się coraz częstszym zjawiskiem. Niektóre firmy zapewniające pomoc techniczną czy agencje rządu USA nie mają nawet biurek dla wszystkich swoich pracowników, gdyż ich środowisko pracy zostało zaprojektowane z myślą o tym, że większość personelu będzie pracować z domu. Zgodnie z dokumentem „Status of Telework Report" (*http://www.telework.gov/Reports_and_Studies/Annual_Reports/2009teleworkreport.pdf*), ponad 100 tysięcy ludzi pracujących w instytucjach rządowych i federalnych pracowało zdalnie w roku 2008, przy czym 64 procent z nich pracowało zdalnie co najmniej od 1 do 3 dni w tygodniu. Dla porównania, ten sam wskaźnik dla roku 2007 wynosił zaledwie 9 procent.

Telepraca oczywiście nie jest zjawiskiem ograniczającym się do Północnej Ameryki. W 39 procentach zachodnioeuropejskich przedsiębiorstw przynajmniej część pracy wykonywana jest zdalnie, zgodnie z raportem „IT and the Environment" opublikowanym w 2007 roku przez Economist Intelligence Unit.

Jednak praca z domu generuje własny zestaw wyzwań, nie ograniczających się do odpowiedzi na pytanie, jak przedsiębiorstwo może zapewnić wsparcie dla środowiska pracy tych osób. Komputerem zlokalizowanym w domu nie można łatwo zarządzać poprzez zasady grupy. W razie awarii nie ma pod ręką personelu, który mógłby natychmiast zapewnić pomoc, zaś osoby pracujące w domu niekoniecznie muszą się biegle orientować w zagadnieniach informatycznych i umieć jasno przedstawić swój problem pracownikom technicznym. Jak wykonać aktualizacje oprogramowania, jeśli, powiedzmy, przyjdzie pora na przejście z Microsoft Office 2007 do Office 2010? Ktoś, kto pracował zdalne nawet przez krótki czas, zapewne zauważył korzyści wynikające z elastyczności i mobilności, ale też wady polegające na braku wsparcia technicznego. Wspaniale jest móc pracować z dowolnego miejsca, choćby kawiarni, hotelu czy poczekalni na lotnisku; bycie swoim własnym helpdeskiem nie jest już takie przyjemne.

Przetwarzanie oparte o serwer ułatwia pracę zdalną na wiele sposobów. Nie musimy martwić się, czy użytkownicy pracujący z domu nie mają zainstalowanych aplikacji, których *nie powinni* uruchamiać na serwerach RDSH, jeśli zastosujemy się do podstawowych procedur bezpieczeństwa (szersze omówienie tego zagadnienia znajdziemy w dalszej części książki). Ponieważ aplikacje rozmieszczone są na serwerach, są instalowane i aktualizowane tutaj, a nie na komputerach klienckich. A jak wspomnieliśmy w poprzednim podrozdziale „Szybkie wyposażanie nowych użytkowników", wykorzystanie RDS pozwala administratorowi na określenie zasobów, które mogą ze sobą współdzielić lokalny i zdalny komputer, a także jakie aplikacje są dostępne zależnie od lokalizacji, z której łączy się użytkownik.

Wprowadzanie Windows do nieprzyjaznych środowisk

Nie wszyscy ludzie, którzy potrzebują komputera osobistego, pracują w środowisku, które pozwala im na korzystanie z niego. Przykładem mogą być firmy elektroniczne. Ktoś tworzący układy scalone pracuje zazwyczaj w tak zwanym *czystym pokoju* – pomieszczeniu chronionym przed kurzem i zanieczyszczeniami, które wymaga czasochłonnego procesu wejściowego. Do takich pomieszczeń nie można wnosić komputerów. Wentylatory wewnątrz

obudowy mogłyby wydmuchiwać na zewnątrz zgromadzony wewnątrz kurz. Ponadto nie byłoby praktyczne korzystanie z komputerów, które mogłyby wymagać obsługi serwisowej, w dowolnym pomieszczeniu, do którego dostęp jest utrudniony ze względu na złożone procedury przygotowawcze. Można jednak wykorzystać w takim miejscu terminale typu *thin client* (ubogi klient) i użyć RDS do udostępniania na nich aplikacji Windows.

Ubogi klient jest też dobrym rozwiązaniem w środowiskach, w których potrzebny jest dostęp do aplikacji Windows, ale okoliczności nie sprzyjają pracy typowych komputerów osobistych, takie jak miejsca o wysokim poziomie zapylenia czy wibracji. Mały terminal, nadający się do montażu na ścianie lub po prostu przenośny, lepiej sprawdza się w takich okolicznościach. Jednak ponieważ takie urządzenia mają bardzo ograniczone zasoby pamięci i procesora, a zazwyczaj w ogóle nie są wyposażone w dyski, nie można na nich uruchomić zaawansowanych systemów, takich jak Windows 7. Aby uzyskać dostęp do najnowszych wersji systemu operacyjnego i aplikacji, potrzebny jest serwer RDSH, z którym terminale będą mogły się łączyć.

Środowiska terminalowe mają zastosowanie też w takich miejscach, jak ekskluzywne kluby fitness czy lobby hotelowe. Zarząd tego typu placówek chciałby zachęcić potencjalnych klientów oferując im możliwość korzystania z komputera, ale niekoniecznie chciałby ponosić koszty obsługi komputerów w takich lokalizacjach. Także ciasnota może być problemem, jeśli próbujemy wcisnąć pięć stanowisk pracy w niewielkim obszarze recepcji. Terminale Windows mogą w takiej sytuacji łączyć się z hostem sesji pulpitu zdalnego i udostępniać aplikacje. Dodatkowo są one mniejsze, wytwarzają mniej ciepła i hałasu i – najogólniej mówiąc – są bardziej niezawodne niż komputery osobiste, które *mogą* być źle skonfigurowane.

Mówi się niekiedy, że inwestowanie w ubogich klientów nie ma sensu, gdyż kupując prawdziwy komputer uzyskujemy większą moc za podobne pieniądze. W przypadku ubogich klientów nie płacimy jednak za moc przetwarzania – tej potrzebujemy bardzo niewiele. Płacimy za możliwość ograniczenia wysiłku administracyjnego, mniejsze rozmiary fizyczne i mniejsze zużycie energii. Rozwiązanie takie nie będzie najlepsze dla każdego, ale niekiedy ubogi klient jest lepszym wyborem niż „pełnoprawny" komputer osobisty.

Ciągłość biznesu i odtwarzanie po awariach

Jedną z głównych zalet RDS jest możliwość szybkiego skonfigurowania środowiska roboczego użytkownika. Dopóki tylko serwery w centrum przetwarzania są sprawne i działają, można je udostępnić użytkownikom w czasie niewiele dłuższym niż potrzebny do wetknięcia wtyczki w komputer użytkownika i jego włączenia. Przy użyciu kombinacji scentralizowanych aplikacji i dostępu do Internetu można przygotować nowe biuro oddziałowe równie szybko, nawet jeśli hosty sesji pulpitu zdalnego będą zlokalizowane w innym miejscu. Dla maksymalnej elastyczności i uproszczenia konfiguracji model ten zakłada, że hosty sesji są niezależne od użytkowników (czyli że wszystkie informacje dotyczące użytkowników, w tym profile, przechowywane są w innym miejscu) i są identycznie skonfigurowane.

Wsparcie dla Green Computing

Jednym z gorących tematów (proszę wybaczyć kalambur) jest obecnie dążenie przedsiębiorstw i rządów do tego, by działać bardziej „zielono" – inaczej mówiąc, jak zużywać mniej energii. IDC, firma badania rynku, informuje, że zużycie energii jest jednym z pięciu najważniejszych problemów, z jakimi borykają się menedżerowie systemów. Przedsiębiorstwa wydają do 10% ogółu budżetu na prąd, jak twierdzi Rakesh Kumar z firmy konsultacyjnej Gartner (jedynie niespełna połowa tej kwoty pokrywa koszty uruchamiania komputera – reszta idzie na ich schładzanie; na każdego dolara wydanego na zasilanie serwera musimy wydać drugiego, by go ochłodzić). Zmniejszenie zużycia energii daje podwójną korzyść – nie tylko redukujemy bezpośrednio wysokość rachunków za prąd, ale dodatkowo ograniczamy zanieczyszczenie środowiska.

> **Uwaga** Opublikowany w grudniu 2007 raport firmy McKinsey & Company „Reducing U.S. Greenhouse Gas Emissions: How Much at What Cost?" (*http://www.mckinsey.com/clientservice/ccsi/pdf/US_ghg_final.report.pdf*) ukazuje uboczne koszty redukcji emisji dwutlenku węgla: saldo kosztów redukcji emisji oraz ogrzewania i zasilania budynków komercyjnych jest ujemne! Tak więc, przedsiębiorstwom *opłaca się* „bycie zielonymi".

W tradycyjnym przetwarzaniu skoncentrowanym na indywidualnych komputerach występuje *wielkie* marnotrawstwo. Zgodnie z danymi IDC, średni poziom wykorzystania serwera wynosi od 15 do 30 procent. Średnie wykorzystanie zasobów dla komputerów indywidualnych szacowane jest na mniej niż 5 procent. Ponieważ pamięć i procesor muszą być zasilane bez względu na to, czy używamy ich, czy nie, jest to marnotrawstwo. Tym samym, zależnie od potrzeb klienta, może być tu całkiem sporo miejsca dla osób uzyskujących dostęp do swoich pulpitów (albo przynajmniej swoich aplikacji) z serwera hosta sesji pulpitu zdalnego. W przypadku firm, które mogą rozsądnie zastąpić komputery biurkowe terminalami Windows może to oznaczać wielkie oszczędności zarówno pod względem mocy zużywanej przez pełnowymiarowe komputery, jak i wymaganej do zasilania klimatyzacji w budynkach podgrzewanych przez setki potężnych komputerów.

Ulepszone wsparcie dla trybu wiersza polecenia

Windows Server 2008 dysponował wielką liczbą programowalnych interfejsów, które powielały – a nawet rozszerzały – możliwości środowiska graficznego. Tym, czego brakowało, była łatwa metoda dostania się do nich. Windows PowerShell zapewniał obsługę Windows Management Instrumentation (WMI0, ale nie dysponował możliwościami zdalnego dostępu (a odnalezienie właściwego obiektu WMI nie jest trywialnym zadaniem, jeśli nie wiemy zawczasu, *czego* szukamy), tak więc nie można było wykorzystać środowiska PowerShell do zarządzania farmą serwerów. VBScript wspiera dostęp zdalny i WMI, ale wymaga umiejętności skryptowania (korzystania z PowerShell też trzeba się nauczyć, ale jest on znacznie prostszy i wiele podstawowych zadań ma już przygotowane polecenia cmdlet).

W systemie Windows Server 2008 R2 zarządzanie z poziomu wiersza polecenia stało się prostsze z dwóch powodów. Po pierwsze, zespół projektowy PowerShell wprowadził

do niego rozwiązania zdalnego dostępu (w wersji 2.0). Po drugie, zespół RDS utworzył obiekty Windows PowerShell mapowane na strukturę WMI usług pulpitu zdalnego. Jest więc możliwe łatwe odszukanie funkcjonalności, której potrzebujemy, stosownie do roli serwera, przy czym obiekty te są w pełni obsługiwane przez standardowe cmdlety PowerShell. W różnych miejscach tej książki będziemy pokazywali, jak wykorzystać Windows PowerShell do zarządzania farmami RDS.

Uwaga Aby zobaczyć przykłady działań, które można realizować przy użyciu Windows PowerShell i RDS, warto zajrzeć do witryny Script Center zespołu RDS pod adresem *http://technet.microsoft.com/en-us/scriptcenter/ee364707.aspx*. Niektóre skrypty wykorzystują VBScript w celu zapewnienia kompatybilności wstecznej z wcześniejszymi systemami operacyjnymi.

RDS w Windows Server 2008 R2: nowe funkcje

Jak dotychczas, pokazaliśmy przegląd niektórych sposobów, które można wykorzystać do przetwarzania opartego na serwerze w celu zaspokojenia potrzeb przedsiębiorstwa, takich jak wsparcie dla zdalnych pracowników lub działania w nieprzyjaznych środowiskach. Wiele nowych funkcji systemu zaprojektowano w celu ułatwienia realizacji takich scenariuszy. Książka ta poświęcona jest głównie poznaniu nowych możliwości RDS i sposobów ich wykorzystania. W tym podrozdziale zajmiemy się niektórymi nowymi funkcjami i tym, jak ta wersja RDS różni się od poprzedników w wymiarze szerszym niż indywidualne funkcje.

Wprost ze źródła

Nowe funkcje RDS, o których zapewne nikt nie słyszał

Greg Shields, RDS MVP

Partner i główny technolog w Concentrated Technology (www.concentratedtech.com)

RDS w Windows Server 2008 R2 jest szeroko dyskutowany w prasie fachowej, gdyż zawiera wiele interesujących nowości. Jednak wśród wyraźnie widocznych usprawnień istnieją też takie, o których mówi się znacznie mniej lub wcale.

Na przykład, czy wiecie, że funkcja *Dynamic Fair Share Schedules* gwarantuje, że każdy użytkownik na danym serwerze uzyskuje równy przydział uwagi procesora? Dzięki temu mało obciążający użytkownik używający programu Word może współdzielić zasoby z intensywnie wykorzystującym zasoby programistą wykonującym kompilację, przetwarzającym wielkie zapytania do baz danych lub dowolne inne działania intensywnie angażujące procesor. Żadna sesja nie jest ograniczana ani „przymulana" przez działania innej.

Remote Desktop IP Virtualization (Wirtualizacja adresu IP serwera usług pulpitu zdalnego) jest również nowością przeznaczoną dla tych wybrednych aplikacji, które wymagają unikatowego adresu IP do działania. Bez niej wszystkie aplikacje uruchomione

na tym samym hoście sesji będą miały ten sam adres IP. Jeśli ją włączymy, serwer RDS może zwirtualizować zestaw adresów IP, aby aplikacje te mogły być wykonywane bez problemów.

Nawet Windows Instaler został usprawniony w wersji Windows Server 2008 R2. We wcześniejszych wersjach Windows Installer nie był w pełni zgodny z usługami terminalowymi. Ograniczenie to sprawiało, że instalowanie niektórych aplikacji było bardzo trudne, gdyż równoległe instalacje mogły blokować się nawzajem. Ta świadomość środowiska jest wreszcie dostępna w R2, zwiększając liczbę udanych instalacji. Instalowanie pakietów MSI na serwerach hosta sesji pulpitu zdalnego odbywa się tak samo jak na komputerze klienckim – są one serializowane i nie ulegają blokowaniu.

Wraz z pojawieniem się wersji R2 opcje łączenia użytkowników z aplikacjami stały się równie ważne jak samo dostarczanie aplikacji. Ta „funkcja" nie jest w istocie funkcją, ale zupełnie nową metodą myślenia o *dostarczaniu aplikacji*. Włączenie rozwiązań RemoteApp i podłączania pulpitu do systemu Windows 7 oraz mechanizm RD Web Access w Windows Server 2008 R2 daje nam więcej sposobów łączenia użytkowników z ich aplikacjami. Zależnie od naszych potrzeb, możemy dostarczać programy RemoteApp i maszyny wirtualne poprzez stronę sieci Web, za pomocą pliku .RDP przesłanego do użytkownika lub (dla tych korzystających z Windows 7), po prostu wpisać je do menu Start użytkowników.

Zmienny charakter wykorzystania hosta sesji

Jedną z istotnych zmian w RDS w Windows Server 2008 R2 są założenia dotyczące zastosowań. W systemie Windows Server 2003 przyjęto założenie, że administratorzy będą (zasadniczo) uruchamiać indywidualne serwery w korporacyjnej sieci lokalnej (i zapewne tylko jeden lub dwa), jako że mechanizmy pośredniczące dostępne były tylko w edycji Enterprise. Projektanci Windows Server 2008 założyli, że serwery terminali będą utrzymywane w farmach, że ludzie będą uruchamiać zarówno aplikacje zainstalowane lokalnie, jak i programy RemoteApp i że przynajmniej niektórzy z nich będą uzyskiwali dostęp do serwerów z Internetu.

RDS w wersji Windows Server 2008 R2 rozszerza założenia poczynione w Windows Server 2008, aby uwzględnić również następujące sytuacje (między innymi):

- Wielu użytkowników uzyskuje dostęp do korporacyjnej sieci z Internetu przynajmniej od czasu do czasu.
- Użytkownicy nie zawsze logują się z komputerów należących do domeny.
- Użytkownicy raczej korzystają z komputerów osobistych (zawierających jakieś lokalnie zainstalowane aplikacje) niż z urządzeń terminalowych.
- Użytkownicy mogą pracować w biurach oddziałowych, ale nadal być przyłączeni do domeny.
- Niektórzy użytkownicy mogą uruchamiać bardzo wymagające aplikacje na serwerach.

- Aplikacje znacznie częściej będą obsługiwane przez farmy identycznych serwerów, niż przez pojedynczy serwer.
- Niektórzy użytkownicy będą mieli prawo do instalowania aplikacji nawet w hostowanym środowisku.
- Niektóre aplikacje powinny być izolowane w celu zapewnienia najlepszej kompatybilności.

Przedstawimy tu nieco informacji o usługach roli RDS, ale techniczne meandry tych funkcji są na razie mniej istotne niż zrozumienie problemów biznesowych, które mają rozwiązywać. W dalszym ciągu tej książki znajdzie się miejsce na omówienie projektowania, wdrażania i wskazówki obsługowe.

Wspieranie użytkowników maszyn wirtualnych

Sesje są dobrą metodą umożliwienia wielu ludziom korzystania z tego samego sprzętu fizycznego. Jednak sesje nie są rozwiązaniem dla każdego, szczególnie wtedy, gdy celem jest całkowita wymiana pulpitu. Sesja nie może dać swoim użytkownikom pełnego dostępu administracyjnego w celu dostrojenia ustawień za pośrednictwem panelu sterowania, nie zawsze jest dobrym środowiskiem dla zasobożernych aplikacji (co więcej, aplikacje takie nie są przyjazne także dla innych sesji) i nie pozwalają użytkownikom na instalowanie aplikacji do późniejszego wykorzystania w dokładnie takim samym środowisku. Nie można też zamrozić sesji, aby łatwo zapisać nie tylko dane, ale także całą pracę, którą wykonujemy, jeśli musimy rzucić wszystko i popędzić na ostatni autobus. Przy użyciu maszyn wirtualnych możemy dokładnie zapisać bieżący stan naszej pracy w dowolnym momencie.

Jedną z nowych funkcji w Windows Server 2008 R2 jest wbudowane wsparcie dla Virtual Desktop Infrastructure (VDI), co w skrócie można nazwać „zarządzanymi maszynami wirtualnymi". Microsoft VDI wspiera dwa rodzaje maszyn wirtualnych. *Osobisty pulpit* (ang. *personal desktop*) jest przypisany do określonej osoby i może być dostosowany zgodnie z dowolnymi regułami wykorzystywanymi w organizacji. *Zbiorcze pulpity* (*pooled desktops*) są ogólnie dostępne dla każdego, kto ma dostęp do puli. Choć w niektórych przypadkach możliwe jest wykonywanie zmian w ich konfiguracji, nie ma gwarancji, że użytkownik logujący się ponownie do zbiorczego pulpitu otrzyma ten sam – wycofywanie zmian jest często standardowym działaniem, aby uniknąć zaśmiecania puli przez aplikacje i ustawienia, których użytkownik nigdy nie użyje ponownie.

Każdy rodzaj pulpitu jest przeznaczony do innych zastosowań. Osobisty pulpit ma całkowicie zastąpić środowisko lokalne. Choć dostępny jest tylko za pośrednictwem RDP, pulpit taki jest kontrolowany przez swojego użytkownika i jeśli jakiś użytkownik ma osobisty pulpit, RD Connection Broker będzie zawsze próbował najpierw połączyć go z tym pulpitem. Jak łatwo zauważyć, osobisty pulpit może zastąpić fizyczny komputer i ma tę dodatkową zaletę, że można bardzo łatwo wykonać kopię zapasową stanu maszyny, zatem przeniesienie go na inną platformę fizyczną nie oznacza utraty wszystkich ustawień.

Zbiorcze pulpity przeznaczone są raczej dla osób, które potrzebują uruchamiać aplikacje nie dające się dobrze utrzymywać na serwerze RDSH, nawet ze wsparciem funkcji równomiernego rozkładania obciążeń, która powstrzymuje pojedynczą sesję przed zużyciem całej mocy przetwarzania procesora. Mogą być one wyposażone we wstępnie zainstalowane aplikacje, których użytkownicy puli mogą potrzebować.

Jak uzyskać RemoteApp od klienta

Technika zdalna jest doskonałym rozwiązaniem, jeśli chodzi o udostępnienie aplikacji, które nie mogą być uruchomione w systemie klienckim. Na przykład możemy uruchomić naprawdę wymagające programy w sesji lub na maszynie wirtualnej, aby zapewnić integrację ze starszym systemem operacyjnym lub zbyt słabym sprzętem.

Zapewnienie wsparcia dla starszych aplikacji, które nie będą działać w systemie operacyjnym nowszym niż Windows Server 2003 i Windows XP, jest nieco bardziej złożone. Windows Server 2003 nie zawiera wsparcia dla technologii RemoteApp, zatem udostępnienie starszej aplikacji oznacza opublikowanie całego pulpitu. A jak dotąd, Windows XP nie wspiera połączeń RemoteApp (choć niektóre firmy stworzyły rozwiązania, które zapewniają zbliżoną funkcjonalność).

Microsoft dysponuje jednak kilkoma różnymi technikami, które pozwalają udostępnić RemoteApp z klienckiego systemu operacyjnego, takiego jak Windows XP. Każda z nich przeznaczona jest dla innych scenariuszy wykorzystania.

XP Mode wykorzystuje technikę Virtual PC do uruchomienia maszyny wirtualnej Windows XP na komputerze systemu Windows 7. Oznacza to, że użytkownicy mogą na swoich własnych komputerach włączyć ten tryb, aby uruchamiać programy niezgodne z Windows 7. Aby pobrać rozwiązanie XP Mode, należy odwiedzić stronę *http://www.microsoft.com/windows/virtual-pc/download.aspx*.

MED-V to – zasadniczo mówiąc – zarządzana wersja XP Mode (*http://blogs.technet.com/medv/archive/2009/04/30/windows-xp-mode-in-windows-y-how-it-relates-to-future--versions-of-med-v.aspx*). Rozwiązania tego można użyć do wdrożenia XP Mode w organizacji, aby nie musieć polegać na poszczególnych użytkownikach w kwestii aktualizacji ich własnych maszyn RemoteApp.

Haczyk, który kryje się w XP Mode, polega na tym, że wymaga, aby maszyna wirtualna RemoteApp była uruchomiona lokalnie. Nie wszystkie komputery dysponują dostatecznie wydajnym sprzętem, aby móc uruchamiać dwa pełne systemy operacyjne jednocześnie, co jest konieczne przy stosowaniu hyperwizora typu 2, takiego jak Virtual PC. Aby zapewnić wsparcie dla RemoteApp z systemu Windows XP, stworzono *RemoteApp for Hyper-V*. W tym modelu system gościa (Windows XP) uruchamiany jest w maszynie wirtualnej na serwerze Hyper-V, zaś do wyświetlenia pulpitu na komputerze systemu Windows 7 wykorzystywany jest protokół RDP. Aktualizacje niezbędne do korzystania z RemoteApp for Hyper-V można pobrać ze strony *http://support.microsoft.com/kb/961742*.

MED-V i XP Mode wykraczają poza zakres tematyczny tej książki, gdyż nie korzystają one z infrastruktury RDS. Natomiast RemoteApp for Hyper-V zostało omówione szczegółowo w rozdziale 3, „Wdrażanie pojedynczego serwera RDSH".

Zbiorcze pulpity mogą również zapewnić wsparcie dla funkcji zgodności aplikacji, która została udostępniona już po opublikowaniu Windows Server 2008 R2: RemoteApp for Hyper-V. Funkcja ta pozwala uruchamiać programy RemoteApp z maszyny wirtualnej, a nie z samego serwera hosta sesji. Została ona zaprojektowana w celu umożliwienia komputerom pracującym pod kontrolą Windows 7 uruchamiania programów, które nie mogą działać

w tym systemie (na przykład aplikacji Web opartej na Internet Explorer 6), przy użyciu komputera systemu Windows XP zlokalizowanego w centrum przetwarzania danych. Choć każda maszyna wirtualna może obsłużyć tylko jedno przychodzące połączenie na raz, RemoteApp for Hyper-V sprawia, że możliwe jest zapewnienie dostępu do tych starszych programów przy jednoczesnym korzystaniu z funkcji Windows 7 na komputerze biurkowym.

Bezpieczna obsługa pracowników zdalnych i mobilnych

Sposoby pracy na polu informacyjnym zmieniły się znacznie w ciągu ostatnich lat. Kiedyś większość pracowników informacyjnych (to chyba najlepszy sposób określenia osób, które regularnie wymagają dostępu do współdzielonych zasobów informacji, aby móc wykonać swoją pracę) szła tam, gdzie były informacje: konkretnie do biura. Opuszczając biuro przerywali każdą pracę zależną od tych scentralizowanych źródeł danych. Analogicznie, dopóki byli w biurze, mogli łatwo dodawać nowe elementy do centralnej puli danych (ostatecznie wszystkie te informacje są tworzone przez ludzi), ale po wyjściu nie mogli już dodać niczego do współdzielonego zbioru informacji.

Pojawienie się laptopów zmieniło sytuację, dając pracownikom komputery, które mogli zabrać ze sobą, ale nawet przenośny komputer nadal nie dawał takiego dostępu do centralnej bazy danych, jaki pracownik miał w biurze. Rozpowszechnienie Internetu w połączeniu z rosnącym wykorzystaniem poczty elektronicznej jako środka komunikacji zapewniły dodatkowy poziom dostępu, ale email nie mógł zawierać *wszystkiego*, co wie firma – jedynie te informacje, które ktoś w nim zamieścił.

Kolejna faza rozwoju obejmowała bezpieczne łączenie się z siecią korporacyjną i pobieranie wymaganych informacji na komputer lokalny. Oczywiście oznaczało to nie tylko konieczność dysponowania dostatecznie szybkim połączeniem, ale również lokalnie zainstalowanymi aplikacjami potrzebnymi do wykonania pracy. Zdradliwym problemem w tym modelu okazało się rozstrzyganie, które komputery mogą łączyć się z siecią korporacyjną i jak utrzymać poufne dane z dala od przenośnych maszyn, które są podatne na kradzież lub zagubienie. Istnieje też problem dostępu do danych, które pracownicy mobilni tworzą podczas podróży. Dane przechowywane na laptopie nie trafią do sieci firmowej, dopóki wędrowiec nie powróci z podróży, a co najmniej będzie on musiał poświęcić sporo czasu, aby przesłać zgromadzone informacje do centralnej puli danych.

RDS od dawna zawierał obietnicę wsparcia dla telepracowników i użytkowników mobilnych, ale rozwiązania zawarte w systemie operacyjnych nie oferowały wszystkich potrzebnych narzędzi, aby mogło to naprawdę działać – aż do publikacji Windows Server 2008. Usługi terminalowe zawarte w tej wersji zmieniły sytuację dzięki wprowadzeniu usługi roli Terminal Services Gateway (Brama usług terminalowych), w skrócie TS Gateway. Mechanizm ten pozwala autoryzowanym użytkownikom na bezpieczny dostęp do zasobów firmowych dzięki tunelowaniu protokołu RDP przez Internet. Windows Server 2008 R2 dodał do tego pewne usprawnienia, zwiększające poziom zabezpieczeń w nowej wersji TS Gateway, obecnie nazywanej Remote Desktop Gateway (RD Gateway).

RD Gateway pozwala użytkownikom na dostęp do sieci korporacyjnej (i scentralizowanej puli danych) poprzez bezpieczne łącza SSL z dowolnego miejsca – hotelu, lotniska, a nawet plaży (o ile tylko będziemy umieli uchronić laptopa przed piaskiem). W połączeniu

z podpisywaniem plików RDP i uwierzytelnianiem serwera RD Gateway zapewnia bezpieczny dostęp przez Internet, dając użytkownikom gwarancję, że plik RDP, który uruchamiają, jest uprawnionym zasobem, a nie fałszywką spreparowaną w celu przechwycenia poświadczeń logowania. RD Gateway może również narzucać zasady chroniące centrum przetwarzania danych, kontrolujące, którzy pracownicy i komputery są uprawnione do tworzenia połączeń określoną drogą i dające administratorom możliwość ustalania, do jakich zasobów mogą uzyskiwać dostęp po nawiązaniu połączenia.

Uwaga RD Gateway i SSL nie są jedynymi metodami tworzenie bezpiecznego połączenia z centrum przetwarzania z lokalizacji zdalnych – nadal dostępne są takie opcje, jak VPN i Direct Access. Jednak RD Gateway ma kilka zalet w porównaniu do konkurencyjnych rozwiązań, w tym możliwość kontroli dostępu na poziomie poszczególnych zasobów, omówioną szczegółowo w rozdziale 10, „Zapewnianie dostępności RDS z Internetu".

Korzystanie z komputerów publicznych bez przechowywania danych połączenia

Osoby często korzystające z dostępu zdalnego zazwyczaj posługują się swoimi własnymi, przenośnymi komputerami. Jednak nie byłoby rozsądne oczekiwać, że ludzie *nigdy* nie będą próbowali logować się z komputera innego niż swój własny. Przeciwnie – zdarza się, że ktoś w trakcie podróży połączy się z serwerem hosta sesji przy użyciu komputera w domu kuzyna w Tucson albo ogólnie dostępnego komputera w kafejce internetowej w Darmstadt. W obu wypadkach trzeba zapewnić dostęp do zasobów roboczych bez buforowania żadnych danych osobistych na tych komputerach, w tym (a nawet zwłaszcza) pliku RDP używanego do zestawienia połączenia.

Remote Desktop Web Access (Dostęp w sieci Web do usług pulpitu zdalnego), w skrócie RD Web Access, dysponuje funkcjami, które umożliwiają osiągnięcie powyższego celu. Zamiast zapisywania ustawień połączenia w pliku RDP, który użytkownik otrzymuje w mailu lub zapisuje na komputerze przenośnym, RD Web Access udostępnia zabezpieczoną witrynę Web, wyświetlającą ikony reprezentujące udostępnione pulpity i programy RemoteApp. Gdy użytkownik kliknie łącze, RD Web Access generuje ustawienia RDP dla wybranego zasobu. Dzięki wprowadzeniu uwierzytelniania opartego na formularzach w systemie Windows Server 2008 R2 użytkownik loguje się w witrynie tylko raz, po czym jego poświadczenia używane są w celu zapewnienia dostępu do wszystkich innych zasobów wyświetlanych w przeglądarce.

RD Web Access i RD Gateway są niezależnymi od siebie usługami roli, ale można je wykorzystywać w dowolnej kombinacji w celu zapewnienia bezpiecznego dostępu z Internetu bez uzależniania się od zapisanych plików RDP.

Integrowanie aplikacji zainstalowanych lokalnie i programów RemoteApp

RDS w Windows Server 2008 R2 nie nakłada specjalnych wymagań na kliencki system operacyjny. Połączenie z maszyną wirtualną lub hostem sesji można uzyskać przy użyciu nawet tak starej wersji programu klienckiego, jak RDP 5.2 (wersje wcześniejsze nie są obsługiwane

ze względu na zmiany modelu zabezpieczeń wprowadzone w wersjach 5.x). Jednak najlepsze efekty uzyskamy używając wersji RDP 7. Ta wersja klienta włącza kilka funkcji wizualnych, które nie były możliwe do zrealizowania w wersjach wcześniejszych. Podobnie jak Terminal Services w Windows Server 2008, RDS jeszcze bardziej zamazuje granicę pomiędzy klientem a serwerem.

Istnieje jedna funkcja RDS, która jest uzależniona od możliwości klienckiego systemu operacyjnego i tym samym jest dostępna tylko dla klientów pracujących pod kontrolą Windows 7: RemoteApp and Desktop Connections (Połączenia programów RemoteApp i pulpitu)[4]. Funkcję tę omówimy szczegółowo w rozdziale 9, „Wdrożenia wieloserwerowe", ale w największym skrócie, umożliwia ona automatyczne dodawanie skrótów do programów uruchamianych na serwerach do menu Start systemu klienckiego.

Uwaga W celu uzyskania najlepszych wrażeń użytkowników powinno się zawsze korzystać z najnowszej wersji programu klienckiego RDP (w momencie pisania tych słów była to wersja 7), jednak wiele funkcji dostępnych jest również dla starszych wersji klienta. Więcej informacji na ten temat zawiera rozdział 6, „Konfigurowanie środowiska użytkowników".

Wsparcie efektów najwyższej jakości za pośrednictwem RDP

Wczesne wersje usług terminalowych ujawniały w oczywisty sposób fakt, że łączymy się z komputerem zdalnym. Jakość obrazu (tryb koloru) była bardzo niska, nie można było przekierować większości urządzeń, można było używać tylko jednego monitora, dźwięk (o ile w ogóle był przekierowywany) był marny i tak dalej.

Windows Server 2008 R2 poprawia wrażenia przy pracy zdalnej dzięki wsparciu dla następujących funkcji:

- Prawdziwa obsługa wielomonitorowości, w tym możliwość zmiany ich rozmieszczenia oraz obsługa zarówno orientacji poziomej, jak i pionowej.
- Zdalny interfejs Aero dla jednomonitorowych sesji w systemie Windows 7.
- Renderowanie multimediów i dźwięku po stronie klienta dla plików Windows Media Player.
- Ulepszone wyświetlanie wideo w formatach Silverlight i Windows Media Foundation.
- Dwukierunkowe przekierowanie dźwięku, łącznie z możliwością nagrywania dźwięku w sesji zdalnej.

Praca z biura oddziałowego

Praca zdalna nie musi dotyczyć wyłącznie tych, którzy pracują w domu lub w trakcie podróży. „Zdalni" pracownicy mogą znajdować się w oddzielnym biurze, ale mieć do dyspozycji podobne zasoby jak w biurze macierzystym. W tym scenariuszu łącze sieciowe jest sprawdzone i niezawodne, komputery są członkami domeny, jednak sama serwerownia nie

4 Użytkownicy wykorzystujący system Windows Server 2008 R2 jako klienta również mogą skonfigurować tę funkcję dla tego systemu.

znajduje się w tej samej lokalizacji co pracownicy, zaś obecny na miejscu personel IT może być minimalny.

Inne przypadki biznesowe

Wśród tych, którzy mogą skorzystać na stosowaniu RDS, znajdują się również administratorzy systemów.

Wymagania zgodności z regulacjami prawnymi

Bezpieczeństwo danych i konieczność zapewnienia zgodności z wymogami prawnymi stanowią najwyższe priorytety dla działów IT w przedsiębiorstwach, które podlegają takim regulacjom. RDS ułatwia zabezpieczanie aplikacji i danych dzięki przechowywaniu ich w centralnej lokalizacji, tym samym redukując ryzyko przypadkowego ujawnienia lub utraty danych z powodu (na przykład) zgubienia laptopa. Kluczowe funkcje RDS, takie jak RD Gateway i RemoteApp, w połączeniu z RD Web Access, pomagają zagwarantować, że firmy współpracujące lub użytkownicy, którzy nie potrzebują pełnego dostępu do sieci firmowej, uzyskają dostęp tylko do tych zasobów, które są im naprawdę potrzebne.

Złożone aplikacje

W środowisku wykorzystującym bardzo złożone aplikacje, takie jak systemy zarządzania przedsiębiorstwem (*line-of-business,* LOB) bądź starsze, dostosowane oprogramowanie, a także w takich sytuacjach, gdy rozbudowane i złożone aplikacje są często aktualizowane i proces ten trudno zautomatyzować, RDS może pomóc w uproszczeniu zarządzania oprogramowaniem. Zamiast konieczności obsługi wielu instalacji w całym środowisku, zarządzana jest pojedyncza instalacja w centrum przetwarzania. Komputery klienckie mogą uzyskiwać dostęp do potrzebnych aplikacji z centralnego źródła bez konieczności instalowania tego oprogramowania lokalnie.

Integracja po fuzjach oraz outsourcing

W przypadku fuzji dwóch przedsiębiorstw konieczne jest zwykle ujednolicenie oprogramowania (na przykład wdrożenie w jednym z nich tej samej aplikacji LOB, która była wykorzystywana w drugiej). Nawet jeśli łączące się firmy korzystały z tego samego oprogramowania, niemal na pewno było ono inaczej skonfigurowane i w innej wersji. Dodatkowo przez pewien czas konieczne jest zachowanie starszej wersji w celu zagwarantowania niezakłóconego dostępu do danych historycznych. Podobnym przypadkiem jest przekierowanie części pracy do firm zewnętrznych, które potrzebują wówczas dostępu do określonych fragmentów LOB, ale nie do całej sieci korporacyjnej. Zamiast wykonywania kosztownego wdrożenia całego zbioru aplikacji LOB w rozszerzonej infrastrukturze, możemy zainstalować te programy na serwerze RDSH i udostępnić je pracownikom i partnerom biznesowym, którzy ich potrzebują.

Wsparcie dla większych farm serwerów

Rzeczywiste wdrożenia RDS nie składają się zazwyczaj z jednego lub dwóch serwerów, jednak narzędzia dostępne w Windows Server 2003 nie zapewniały prawdziwego wsparcia dla farm (komponent Session Directory Server był dostępny tylko w edycji Enterprise). System Windows Server 2008 R2 jest znacznie lepiej wyposażony, jeśli chodzi o zarządzanie dostępem do wielu serwerów, gdyż włączono w nim dodatkowe zasady grupy umożliwiające zarządzanie serwerami oraz komponent RD Connection Broker (Broker połączeń usług pulpitu zdalnego), pozwalający użytkownikom na uzyskiwanie połączenia z farmami serwerów, zamiast pojedynczych maszyn.

Nowe rozwiązania RDS w Windows Server 2008 R2

Nowe rozwiązania zawarte w RDS znacząco poprawiają wrażenia użytkowników. Jednym z celów tego wydania było sprawienie, aby przetwarzanie zdalne było możliwie dyskretne – innymi słowy, aby aplikacja wykonywana zdalnie wyglądała tak samo jak uruchomiona lokalnie. W tym podrozdziale przedstawimy niektóre rozwiązania, które to umożliwiają, zaś szczegółowe omówienie znajduje się w dalszej części książki.

Integracja programów RemoteApp w menu Start

Z technicznego punktu widzenia, zintegrowanie skrótów do programów RemoteApp z menu Start było możliwe już w Windows Server 2008. W tym celu należało wykonać następujące działania:

1. Utworzyć pakiet instalatora Windows (MSI) dla aplikacji RemoteApp z hosta sesji pulpitu zdalnego.
2. Opublikować ten plik MSI za pośrednictwem Zasad grupy.
3. Przepakować aplikację i ponownie opublikować ręcznie, gdy ustawienia RemoteApp ulegną zmianie.

Nie jest to złe rozwiązanie i publikowanie MSI nadal jest jedynym sposobem, którym możemy obsłużyć powiązania plików z programami RemoteApp (jest to również jedyny sposób integracji programów RemoteApp z systemami Windows XP i Windows Vista). Nie zapewnia jednak automatycznej aktualizacji ani dodawania nowych programów do menu Start bez edytowania Zasad grupy. A przede wszystkim, ponieważ rozwiązanie to jest zależne od zasad grupy, nie możemy wykorzystać tej metody do udostępniania aplikacji dla komputerów, które znajdują się poza domeną.

Nowa funkcja o nazwie RemoteApp and Desktop Connections (Połączenia programów RemoteApp i pulpitu) pozwala ominąć te ograniczenia. Nowy element panelu sterowania w systemie Windows 7 (dostępny także w Windows Server 2008 R2) akceptuje URL dla strumienia publikacji (*publishing feed*) utworzonego dla farmy. Strumień ten scala wszystkie dostępne programy RemoteApp, pule maszyn wirtualnych i osobiste pulpity. Gdy użytkownik łączy się z podanym adresem URL i przedstawi wymagane poświadczenia, RD Web Access filtruje wyświetlane elementy, dzięki czemu użytkownik otrzyma łącza tylko do tych zasobów, do których ma uprawnienia. Łącza te są umieszczane w menu Start systemu klienckiego.

Zastosowanie RemoteApp and Desktop Connections zapewnia następujące korzyści:

- Pozwala użytkownikom na uruchamianie programów zainstalowanych lokalnie i programów RemoteApp w taki sam sposób – poprzez łącza w menu Start.
- Nie wymaga przyłączania komputera do domeny.
- Łącza są aktualizowane automatycznie, gdy programy RemoteApp lub maszyny wirtualne są dodawane lub usuwane ze strumienia albo gdy zmienią się uprawnienia.
- Użytkownicy muszą logować się tylko raz, aby utworzyć połączenie.
- Na koniec strumień jest zapisany w formacie XML, co pozwala programistom na wykorzystanie go innymi sposobami.

Przekierowanie trybu Aero Glass

Jednym z najbardziej widocznych ograniczeń usług terminalowych w Windows Server 2008 był fakt, że Windows Vista dysponowały wspaniałym interfejsem Aero Glass... ale nie był on dostępny w sesjach terminalowych. Obecnie przekierowywanie Aero jest dostępne przy połączeniach z maszynami wirtualnymi Windows 7 i sesjami Windows Server 2008 R2 z komputerów klienckich systemu Windows 7 – nawet w sytuacji, gdy punkt końcowy nie był w stanie sam wyświetlić interfejsu Aero (na przykład przy łączeniu się z komputerem pozbawionym podsystemu wideo – *headless computer*).

Przekierowanie Aero Glass z systemu Windows 7 jest włączone domyślnie; aby włączyć je w systemie Windows Server 2008 R2, należy wykonać dostrojenie kompozycji pulpitu. Szczegółowe omówienie tego zagadnienia zawiera rozdział 6.

> **Uwaga** Jakkolwiek możliwe jest uzyskanie przekierowania Aero z Windows Vista do innego komputera Windows Vista, przekierowanie Aero z Windows 7 lub Windows Server 2008 R2 wymaga Windows 7 jako klienckiego systemu operacyjnego.

Przekierowanie Aero Glass jest możliwe tylko dla sesji wykorzystujących pojedynczy monitor.

Ulepszona zgodność aplikacji

Jednym z istotnych pytań dotyczących aplikacji, szczególnie tych, które są bardziej wymagające, jest to, czy będą one mogły działać na serwerze hosta pulpitu zdalnego. W systemie Windows Server 2008 R2 istnieją trzy nowe rozwiązania, które pozwalają rozwiązać problemy kompatybilności aplikacji:

- Zmiany w procesie instalowania pakietów MSI sprawiają, że instalacja przebiega podobnie jak w klienckich systemach operacyjnych. Szczegółowe omówienie tych zagadnień zawiera rozdział 3, jednak tu możemy zauważyć, że pozwalają one uniknąć wzajemnego blokowania się wystąpień aplikacji podczas pierwszego uruchamiania.
- Windows Server 2008 zawierał komponent Windows System Resource Manager (WSRM), ograniczający możliwość zużycia całego czasu procesora przez pojedynczą sesję lub proces. Mechanizm ten jest nadal dostępny w Windows Server 2008 R2, ale system ten zawiera nową funkcję, eliminującą takie problemy w bardziej proaktywny sposób.

Podczas gdy WSRM wykrywa „złe zachowanie” aplikacji i ogranicza im przydział czasu procesora, Dynamic Fair Share Scheduling (DFSS) wykorzystuje mechanizm harmonogramu w celu zagwarantowania, że pojedyncza sesja nie pozbawi innych sesji należnych im cykli procesora. Szersze omówienie tego mechanizmu zawiera rozdział 3.

- Wirtualizacja adresu IP umożliwia przydzielenie dla sesji – a nawet dla określonej aplikacji uruchomionej w danej sesji – unikatowego adresu IP. We wcześniejszych wersjach usług terminalowych wszystkie aplikacje uruchomione na serwerze używały tego samego adresu IP: adresu serwera. Jakkolwiek działa to poprawnie w większości wypadków, uniemożliwiało to działanie niektórych aplikacji lub konfiguracji zabezpieczeń, które wymagały oddzielnych adresów. Także to zagadnienie omówione jest w rozdziale 3.

Wsparcie dla rzeczywistej wielomonitorowości

Wersja 6 klienta pulpitu zdalnego (RDC) wprowadziła rozszerzanie monitora, przez co możliwe było wykorzystanie dwóch lub więcej monitorów (aż do łącznej rozdzielczości 4096 x 2048) do wyświetlania sesji zdalnej. W tym celu należało łączyć się z serwerem terminali przy użyciu przełącznika */span*. Było to usprawnienie w porównaniu do wcześniejszego ograniczenia do pojedynczego monitora, ale miało kilka wad:

- Monitory musiały być ustawione obok siebie („w rzędzie”).
- Sesja zdalna była nadal sesją jednomonitorową – jedynie z *bardzo* wielkim monitorem. Oznaczało to, że przy korzystaniu z dwóch monitorów komunikaty systemowe i inne okna dialogowe, domyślnie pozycjonowane na środku, wypadały na „złączeniu” monitorów, przez co były nieczytelne i niewygodne. Dodatkowo maksymalizacja aplikacji powodowała zajęcie całej dostępnej przestrzeni (wszystkich monitorów).

Całkowita obsługiwana rozdzielczość musiała mieścić się w zakresie do 4096 x 2048 (na przykład 1600 x 1200 + 1600 x 1200 = 3200 x 1200).

RDS zastępuje rozszerzanie monitora przez prawdziwą obsługę wielu monitorów. W tym przypadku każdy monitor maszyny klienckiej jest przekierowywany niezależnie, zatem każdy z nich (do 16) jest widoczny jako oddzielny wyświetlacz dla sesji zdalnej (Zasady grupy ograniczają liczbę monitorów do 10, ale jest technicznie możliwe podniesienie tej wartości do 16, jeśli narzucimy tę wartość programowo). Tym samym:

- Monitory mogą być rozmieszczone w dowolny sposób, który ma sens dla użytkownika: w wierszu, w pionie, jako litera L i tak dalej.
- Poszczególne aplikacje podczas maksymalizowania dopasowują się do tego monitora, na którym są aktualnie wyświetlane, a nie do całego zbiorczego zestawu.
- Każdy monitor może mieć rozdzielczość do 4096 x 2048.

Rzeczywista wielomonitorowość nie jest obsługiwana przy przekierowaniu Aero Glass. Jeśli zostaną skonfigurowane obie funkcje, pierwszeństwo ma wielomonitorowość.

Przekierowywanie wielkich wyświetlaczy w wysokiej rozdzielczości może mieć znaczący wpływ na wydajność serwera, zatem zalecane jest dopasowanie maksymalnej obsługiwanej rozdzielczości i maksymalnej liczby monitorów. Więcej szczegółów na ten temat zawiera rozdział 6.

Renderowanie multimediów po stronie klienta

Wiele dzisiejszych komputerów osobistych, nawet te stosunkowo skromne, ma wielką moc – znacznie większą, niż serwer mógłby udostępnić do renderowania multimediów w sesji, nie wspominając o konieczności strumieniowania tych danych do klienta.

W systemie Windows Server 2008 R2 zespół projektowy RDS usprawnił odtwarzanie mediów poprzez wydajne transportowanie danych audio/wideo w skompresowanym formacie wewnątrz protokołu RDP. Zamiast przetwarzania tych danych na serwerze, przesyłane są one do klienta i dopiero tam odtwarzane przy użyciu Windows Media Player. Zawartość wygląda zatem na wyświetlaną lokalnie – i tak jest w istocie, nawet jeśli została oryginalnie wygenerowana w sesji zdalnej. Nadal jednak jest w pełni zintegrowana z sesją zdalną.

Podejście to daje kilka korzyści:

- Redukuje wykorzystanie pasma sieciowego, gdyż dane przesyłane są skompresowanymi danymi wideo, a nie serią następujących po sobie bitmap. Wrażenie jest podobne do odtwarzania pliku z udziału sieciowego lub serwera wideo. Co więcej, zmiana wielkości okna nie wpływa na odtwarzanie zawartości.
- Zmniejszone zostaje przetwarzanie na serwerze, gdyż serwer nie musi wykonywać dekodowania wideo i pakować go w protokół RDP.

Funkcja ta wymaga wsparcia dla przekierowania multimediów po stronie klienta oraz skonfigurowania serwera do odtwarzania dźwięku i wideo. Szersze omówienie tej funkcji zawiera rozdział 6.

Pojedyncze logowanie do farmy

Mechanizm pojedynczego logowania, czyli konieczność podawania hasła tylko raz, bez wątpienia jest wygodny z punktu widzenia użytkownika. Wyobraźmy sobie, że zaczynamy pracę i logujemy się do komputera. Następnie klikamy ikonę jakiegoś programu i musimy zalogować się ponownie. Później chcemy otworzyć jakiś plik – i znów pojawia się pytanie o użytkownika i hasło. Jeśli zamkniemy aplikację i uruchomimy ją ponownie, znów trzeba będzie się zalogować... Przed upływem godziny wolelibyśmy raczej rzucić wszystko i zapomnieć o pracy, gdyż w tych warunkach po prostu nie da się pracować produktywnie!

Pojedyncze logowanie zostało wprowadzone w systemie Windows Server 2008, ale zostało dodatkowo usprawnione w Windows Server 2008 R2 dzięki uwierzytelnianiu opartym na formularzach. Podczas gdy wcześniejsza wersja pozwalała kontynuować pracę bez ponownego podawania poświadczeń, o ile łączyliśmy się z tym samym serwerem, obecnie poświadczenia są buforowane w zabezpieczonym formularzu Web i przesyłane w tle do serwera za każdym razem, gdy podejmiemy próbę dostępu do programu RemoteApp.

Rozszerzenie mechanizmu łatwego drukowania na platformy klienckie i eliminowanie zależności od .NET

Sterowniki drukarek od dawna były zmorą administratorów serwerów terminali. Po pierwsze, obsługiwanie sterowników było grą, w której wygrana polegała na tym, że sterownik nie powodował padu serwera. Wspieranie drukarek po stronie klienta zwiększało wystawienie systemu na ryzyko wadliwego sterownika, jako że administratorzy mieli mniejszą kontrolę

nad instalowanymi sterownikami. Przy obsłudze sterowników Windows NT na serwerze terminali i innych po stronie klienta (na przykład przy korzystaniu z klienta Windows 98 i serwera Windows 2000 Server) sterowniki mogły nawet używać odmiennych nazw. Oznaczało to konieczność tworzenia plików mapowania sterowników, które zasadniczo informowały „gdy system odwołuje się do *tego* sterownika w sesji klienckiej, należy użyć *tamtego* na serwerze terminali". W przeciwnym wypadku zadanie wydruku kończyło się niczym (w najlepszym razie).

Z upływem czasu sterowniki stawały się bardziej niezawodne, jako że problem był coraz lepiej rozumiany. Gdy zarówno system kliencki, jak i serwer terminali używa technologii Windows NT, problem niezgodności nazw sterowników przestał występować. W Windows Server 2003 pojawiła się nowa zasada grupy, która pozwalała domyślnie tylko na sterowniki trybu użytkownika. Wyeliminowało to ryzyko instalacji źle napisanego sterownika trybu jądra, który mógłby wysadzić system w powietrze, ale nadal administratorzy musieli testować, utrzymywać i zapewniać wsparcie dla najrozmaitszych sterowników dla drukarek firmowych i mapowanych drukarek klienckich (choć niektóre firmy zrezygnowały z wspierania mapowanych drukarek klienckich, po prostu w celu uniknięcia problemów).

Innym problemem występującym we wcześniejszych rozwiązaniach drukowania było decydowanie, które drukarki powinny być mapowane do sesji zdalnej. Jeśli mapowanie drukarek było włączone, wszystkie drukarki podłączone po stronie klienta były widoczne dla serwera terminali, bez względu na to, czy było to uzasadnione. Mapowanie tych wszystkich drukarek było też czasochłonne, nie wspominając o zwiększonej liczbie sterowników, które musiały być zainstalowane na serwerze terminali.

Terminal Services w systemie Windows Server 2008 pozwalały rozwiązać te problemy na dwa sposoby. Pierwszy (i najprostszy) to Zasada grupy, która pozwalała administratorom włączyć mapowanie w sesji zdalnej tylko *domyślnej* drukarki klienta. Drugim jest mechanizm Easy Print (Łatwe drukowanie), eliminujący problemy sterowników, o ile klient wykorzystuje system Windows Vista i RDC 6.1. Zasadniczo Easy Print pozwala użytkownikom drukować z sesji zdalnej bez konieczności instalowania jakichkolwiek sterowników na serwerze terminali. Sesja zdalna pobiera ustawienia drukarki z systemu klienckiego i nawet wykonuje wywołania do interfejsu po stronie klienta, aby wyświetlić okno konfiguracji sterownika.

Easy Print miał jednak również wady: nie działał przy połączeniach z innymi systemami klienckimi (co eliminuje najczęstsze scenariusze typu VDI) i wymagał instalacji .NET w systemie operacyjnym klienta, aby działać. W Windows Server 2008 R2 obydwa ograniczenia zostały usunięte. Podczas gdy .NET był wymagany do konwersji strumienia danych XPS na komendy GDI konieczne do drukowania, zarówno w Windows Server 2008 R2, jak i w Windows 7 operacje te są wykonywane przez sam system operacyjny. Więcej informacji na temat Easy Print zawiera rozdział 6.

Role RDS w Windows Server 2008 R2

Użytkownicy, którzy znają mechanizm usług terminalowych w Windows Server 2008, łatwo zauważą, że większość ról związanych z RDS w Windows Server 2008 R2 wygląda znajomo. RDS jest obsługiwany przez sześć usług roli:

- RD Session Host (Host sesji usług pulpitu zdalnego)

- RD Virtualization Host (Host wirtualizacji pulpitu zdalnego)
- RD Connection Broker (Broker połączeń usług pulpitu zdalnego)
- RD Web Access (Dostęp w sieci Web do usług pulpitu zdalnego)
- RD Gateway (Brama usług pulpitu zdalnego)
- RD Licensing (Licencjonowanie usług pulpitu zdalnego)

RD Session Host

Remote Desktop Session Host (w systemie Windows Server 2008 nazywany serwerem terminali) pozostaje podstawowym składnikiem architektury RDS, dostarczającym indywidualne aplikacje i zapewniającym największą gęstość użytkowników pełnych pulpitów. Serwer RDSH różni się od innych funkcjonalności serwerów Windows pod wieloma względami. Zasadniczo, serwer z zainstalowaną tą rolą działa bardziej jak stacja robocza, niż jak serwer.

Przykładowo, inne role serwera zostały zaprojektowane do obsługi jednego ogólnego celu, takiego jak dostarczanie poczty elektronicznej lub wykonywanie zapytań do bazy danych. Ich priorytety są jasne: cokolwiek jest wykonywane na pierwszym planie celu tego serwera, otrzymuje lwią część mocy procesora. Serwer udostępniany działa inaczej. Wiele osób wykorzystuje go w tym samym czasie, zatem nie można zakładać, która aplikacja jest na pierwszym planie, a które w tle – którą z czterdziestu równoległych sesji powinien wybrać? Tym samym wszystkie procesy użytkowników na hoście sesji mają ten sam priorytet, dzięki czemu uzyskujemy mniej więcej równomierny podział mocy przetwarzania pomiędzy wszystkich zdalnych użytkowników.

> **Uwaga** W systemie Windows Server 2008 R2 dostępna jest nowa funkcja o nazwie Dynamic Fair Share Scheduling (DFSS), która aktywnie kontroluje przydzielanie czasu procesora dla poszczególnych sesji i gwarantuje, że żadna z nich nie zawłaszczy całej mocy przetwarzania. Funkcja ta jest domyślnie włączona.

Użytkownicy łączą się z hostem sesji za pośrednictwem protokołu RDP (Remote Desktop Protocol). Konfiguracja połączenia zapisywana jest w pliku RDP, którego wywołanie powoduje uruchomienie programu klienckiego i połączenie. Plik taki użytkownik może pobrać z udziału sieciowego lub otrzymać w wiadomości email, a także może on zostać automatycznie wygenerowany w przeglądarce lub (w przypadku systemu Windows 7) w menu Start za pośrednictwem mechanizmu RemoteApp and Desktop Connections. Gdy użytkownik rozpoczyna sesję zdalną, jest ona odseparowana od innych sesji zdalnych uruchomionych na tym samym komputerze. Użytkownicy nie widzą innych sesji, zaś aplikacje uruchomione w tych sesjach nie współdzielą pamięci dostępnej do zapisu. Sesja może mieć pewien nieświadomy wpływ na inne sesje (na przykład przy korzystaniu z wymagających aplikacji, które rezerwują wielkie obszary pamięci), ale ryzyko zabezpieczeń związane z faktem, że wielu użytkowników jednocześnie uruchamia sesje na tym samym hoście, jest minimalne. Nie możemy oczywiście powiedzieć, że „nie ma zagrożenia", gdyż istnieją pewne wyjątkowe sytuacje, które mogłyby zostać nadużyte przez eksperta dysponującego odpowiednimi narzędziami, ale najogólniej jest to prawda.

Najlepsze rozwiązanie Serwery RDSH zazwyczaj mają bardzo duże obciążenie związane z obsługą wszystkich sesji zdalnych, zatem powinny być przeznaczone tylko do tego celu i nie pełnić żadnych dodatkowych funkcji.

Rozdział 2, „Kluczowe koncepcje architektury RDS", zawiera wskazówki dotyczące wymiarowania serwera hosta sesji. Informacje na temat instalowania i konfigurowania roli zamieszczone są w rozdziale 3, zaś tworzenie farm serwerów z użyciem RD Connection Broker omówione jest w rozdziale 9.

RD Virtualization Host

Windows Server 2008 R2 wprowadza nowy typ obsługiwanego zasobu: maszyny wirtualne, w skrócie VM (Virtual Machine). Oczywiście sama technologia maszyn wirtualnych nie jest nowością, ale ich wsparcie w infrastrukturze RDS – tak. Ta usługa roli wykorzystuje Hyper-V do utrzymywania maszyn wirtualnych. Maszyny te mogą być rozmieszczone w puli (dostępne dla każdego, kto ma dostęp do puli) lub osobiste (przypisane do konkretnego użytkownika Active Directory).

Po co potrzebne jest wsparcie dla maszyn wirtualnych *obok* sesji? Odpowiedź jest prosta: obydwie są skutecznymi sposobami wirtualizacji pulpitu. Jeśli chcemy osiągnąć większą gęstość (czyli większą liczbę równoczesnych użytkowników), użyjemy sesji. *Znacznie więcej* osób może jednocześnie pracować używając sesji na pojedynczym komputerze, niż maszyn wirtualnych, gdyż sesje współdzielą znaczącą część podstawowej infrastruktury systemu operacyjnego (mimo że nie widzą się nawzajem). VM jest wirtualną manifestacją maszyny fizycznej, a tym samym poszczególne maszyny są całkowicie odseparowane od siebie. Wymaga to jednak znacznie większych zasobów. Serwer z pamięcią wynoszącą 4 GB i nowoczesnym procesorem pozwoli na uruchomienie kilkunastu równoległych sesji, ale ten sam serwer z trudem poradzi sobie z obsługą więcej niż dwóch czy trzech maszyn wirtualnych w tym samym czasie.

Uwaga To zdarzyło się naprawdę: na pewnym spotkaniu dotyczącym wirtualizacji niektórzy uczestnicy oświadczyli, że słyszeli już o wirtualizacji pulpitów przy użyciu VM, ale nigdy nie słyszeli o sesjach i byli bardzo zainteresowani możliwościami „lekkiego VDI".

Powód, dla którego VM mogą być przydatne, jest ściśle związany z tym, dlaczego są tak wymagające: stanowią całkowicie odizolowane środowisko. VM ma przydzieloną określoną wielkość pamięci i liczbę procesorów, zarezerwowanych dla niej i niedostępnych dla innych maszyn wirtualnych (a nawet – w pewnym stopniu – dla systemu hosta). System operacyjny również jest oddzielny i przeznaczony wyłącznie do obsługi tej maszyny. Oznacza to, że cokolwiek się wydarzy wewnątrz VM, nie ma żadnego wpływu na inne maszyny wirtualne działające na tym samym serwerze fizycznym. Użytkownicy mogą uruchamiać najbardziej nawet wymagające programy, takie jak CAD, i nie ograniczą zasobów innych maszyn wirtualnych. Użytkownik może też dowolnie popsuć konfigurację swojej maszyny wirtualnej, doprowadzając ją do awarii, ale wpłynie to tylko na niego samego.

W architekturze RDS maszyny wirtualne są zwykle przypisywane użytkownikom o szczególnie dużych wymaganiach. Ci, którzy otrzymują osobiste pulpity, to ci, którzy potrzebują pełnego zastąpienia możliwości indywidualnego komputera (ale z możliwością scentralizowanego tworzenia kopii zapasowych i poziomem bezpieczeństwa zapewnianym przez centrum przetwarzania danych). Pulpity osobiste są też dobrymi kandydatami dla aplikacji, które wymagają stałego, lokalnego źródła danych (czyli takich, które nie mogą przechowywać swoich danych w udziale sieciowym). Z kolei zbiorcze pulpity przeznaczone są dla użytkowników, którzy potrzebują aplikacji nie dających się łatwo (lub wcale) zwirtualizować na hoście sesji pulpitu zdalnego z jakiegokolwiek powodu – na przykład wymagają starszej wersji przeglądarki, są 16-bitowe (Windows Server 2008 R2 występuje wyłącznie w wersji 64-bitowej i nie ma możliwości uruchamiania w nim programów 16-bitowych) albo z jakiegoś innego powodu nie pasują, ale mogą działać na zbiorczej maszynie wirtualnej.

Dobieranie sprzętu i mocy dla RD Virtualization Host omówione jest w rozdziale 2. Rozdział 4, „Wdrażanie pojedynczego serwera RD Virtualization Host", przedstawia instalację roli w wersji jednoserwerowej, zaś wdrożenie jej na farmie serwerów znajdziemy w rozdziale 9. Rozdział 10 zawiera omówienie zarządzania większymi wdrożeniami.

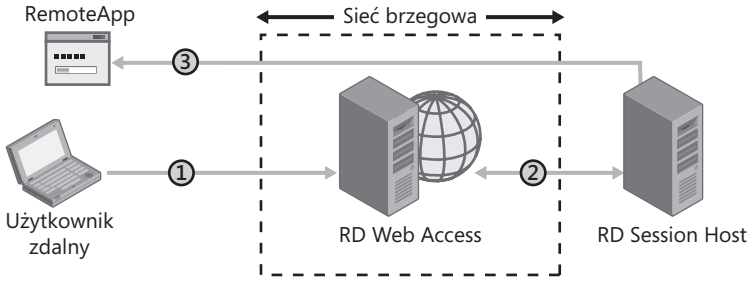
RD Web Access

Remote Desktop Web Access (Dostęp w sieci Web do usług pulpitu zdalnego) współdziała z Microsoft Internet Information Services (IIS), umożliwiając wyświetlenie ikon autoryzowanych programów RemoteApp i maszyn wirtualnych w portalu i samoczynnie tworząc połączenie. Użytkownik loguje się w portalu i może zobaczyć ikony dla wszystkich zasobów zdalnych przydzielonych mu przez administratora. Gdy kliknie ikonę, portal tworzy połączenie i uruchamia program RemoteApp w bardzo podobny sposób, jakby był uruchamiany za pośrednictwem pliku RDP. Przy użyciu nowego mechanizmu uwierzytelniania opartego na formularzach użytkownik musi logować się tylko raz – później jego poświadczenia są używane dla wszystkich zasobów, do których ma przydzielony dostęp.

W momencie uruchomienia programu RemoteApp na serwerze RDSH uruchamiana jest sesja utrzymująca ten program. Analogicznie, kliknięcie ikony symbolizującej VM uruchamia odpowiednią maszynę wirtualną. Sam serwer RD Web Access nie uruchamia ani nie utrzymuje aplikacji. Jak widać na rysunku 1-1, jedynie wyświetla on ikonę aplikacji, tworzy plik RDP w momencie podwójnego kliknięcia (1) i przekazuje ten plik użytkownikowi, aby uruchomić aplikację na serwerze hosta sesji (2). Programy RemoteApp lub pulpity uruchomione w ten sposób nie są wyświetlane w przeglądarce, ale w swoich własnych oknach (3) i są niezależne od okna przeglądarki. Zamknięcie przeglądarki nie powoduje rozłączenia ani nie zamyka łącza pomiędzy klientem a hostem sesji lub maszyną wirtualną.

RD Web Access przynosi wiele korzyści, w tym:

- Użytkownicy mogą uzyskiwać dostęp do programów RemoteApp z witryny widocznej w Internecie lub intranecie. Aby uruchomić program, muszą tylko podwójnie kliknąć jego ikonę.
- Dzięki nowej funkcji jednokrotnego logowania, po uwierzytelnieniu użytkownika w witrynie jego poświadczenia są buforowane i przekazywane do każdego nowo tworzonego połączenia – także z innymi serwerami lub farmami.



Rysunek 1-1 RD Web Access wyświetla ikony aplikacji w przeglądarce, ułatwiając użytkownikom dostęp do zasobów serwera.

- RD Web Access może zawierać zasoby z więcej niż jednej farmy i łączyć je w jednym oknie.
- RD Web Access wyświetla tylko te zasoby, które są przypisane do konkretnej osoby.
- Dzięki wykorzystaniu RD Web Access znacznie zmniejsza się obciążenie administracyjne, związane z utrzymywaniem i dystrybucją plików RDP obsługujących połączenia z farmą hostów sesji. Można łatwo wdrożyć programy w centralnej lokalizacji i nie trzeba się zajmować aktualizacją plików zawierających dane połączenia.
- RD Web Access zawiera komponent Remote Desktop Web Connection (Podłączanie pulpitu zdalnego w sieci Web), który pozwala użytkownikom na łączenie się zdalne z dowolnego komputera, który może nawiązać połączenie z portalem RD Web Access.
- RD Web Access wymaga tylko minimalnej konfiguracji, ale tworzona przez niego strona Web zawiera dostosowywalny składnik Web Part, który można dołączyć do niestandardowej strony lub witryny Microsoft SharePoint.

Z tych powodów RD Web Access jest korzystny dla osób używających przeglądarki... ale w Windows Server 2008 R2 ta usługa roli wspiera nawet osoby łączące się bez pośrednictwa przeglądarki. RemoteApp and Desktop Connections jest nową funkcją systemu Windows 7 (jest to część systemu operacyjnego, nie zaś klient RDP, zatem nie jest dostępna we wcześniejszych wersjach Windows), która umożliwia dołączenie ikon programów RemoteApp i maszyn wirtualnych do menu Start systemu klienckiego i uruchamiania ich stamtąd. Sztuczka polega na tym, że RD Web Access uzyskuje informacje, jakie programy i zasoby są dostępne dla poszczególnych użytkowników, z usługi publikowania RD Connection Broker i sprawia, że zasoby te są dostępne poprzez URL. Jeden URL wskazuje witrynę, którą możemy zobaczyć w przeglądarce, a inny wspiera łącza dostarczane do mechanizmu RemoteApp and Desktop Connections.

RD Connection Broker

Ze względu na potrzebę nadmiarowości i równoważenie obciążenia, dobra praktyka wymaga instalacji więcej niż jednego serwera RDSH, utrzymującego zestaw aplikacji zdalnych. To samo, a nawet jeszcze silniej, dotyczy maszyn wirtualnych – jeśli potrzebujemy więcej niż jednej lub dwóch, niemal zawsze będziemy potrzebować więcej niż jednego serwera RD Virtualization Host.

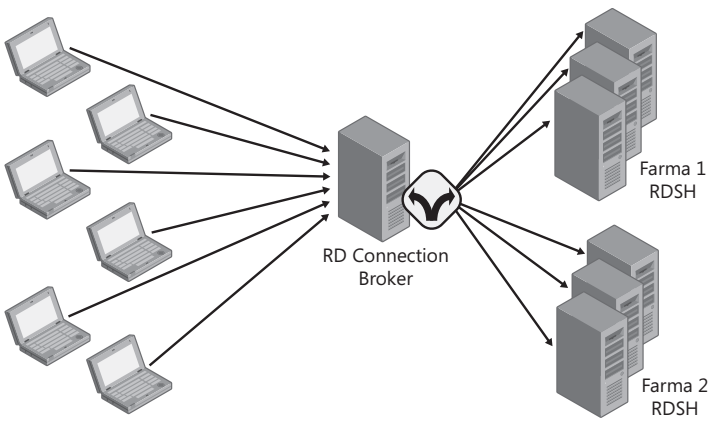
Dysponując wieloma punktami końcowymi i serwerami, które je obsługują, pozwala rozproszyć obciążenie i wyeliminować ryzyko, że jeśli jedyny serwer zostanie wyłączony, zostaniemy pozbawieni możliwości obsługi scentralizowanych aplikacji. Problem w tym, że połączenia są zasadniczo tworzone do indywidualnych serwerów hosta sesji, a nie do ich grup. Tak więc finalne połączenie zawsze trafia do jakiegoś określonego serwera.

Jeśli jednak pliki RDP zawierałyby nazwy indywidualnych serwerów, nie byłoby możliwe równoważenie obciążenia ani przekazanie przychodzących połączeń w razie awarii. Nie dawałyby też dostatecznej elastyczności, aby ustalić, że dany użytkownik powinien zostać przełączony do innego serwera, gdy uruchamia nową aplikację, gdyż ma już ją otwartą na tym serwerze. Jeśli wykorzystujemy maszyny wirtualne, możemy przekierować plik RDP do tej konkretnej VM bez wykonywania żadnych przypisań w Active Directory – połączenie z maszyną wirtualną nie różni się niczym od wykorzystania RDP do połączenia z konkretnym komputerem fizycznym identyfikowanym przez nazwę. Jednak przypisywanie VM poprzez nazwy nie pozwoli nam korzystać ze zbiorczych pulpitów. Co więcej, plik RDP nie będzie mógł automatycznie obudzić VM z hibernacji i przygotować jej do połączenia. Jeśli podejmiemy próbę bezpośredniego połączenia z zahibernowaną maszyną wirtualną, połączenie się nie powiedzie.

Jak to działa

Wprowadzenie do rozdzielania połączeń

Usługa roli RD Connection Broker rozwiązuje problem przydzielania połączeń dla żądań użytkowników, inteligentnie kierując je do właściwego punktu końcowego, jak pokazano na rysunku 1-2.



Rysunek 1-2 RD Connection Broker przekierowuje połączenie do odpowiedniego serwera hosta sesji.

W przypadku aplikacji RemoteApp RD Connection Broker podejmuje decyzję na podstawie kilku kryteriów, w tym:

- Do jakiej farmy kierowane było przychodzące żądanie połączenia?

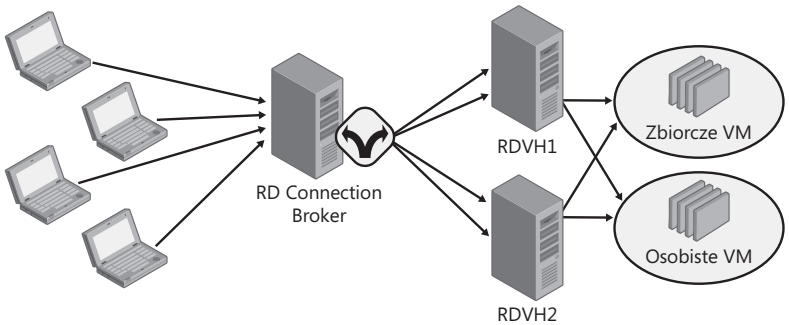
Ciąg dalszy na stronie następnej

- Czy osoba wykonująca żądanie ma już (aktywną lub rozłączoną) sesję w tej farmie?
- Jeśli nie istnieje połączenie, który serwer ma najmniejszą liczbę aktywnych sesji?

W przypadku połączeń VM (rysunek 1-3) RD Connection Broker wykorzystuje zbliżone kryteria:

- Czy żądanie dotyczy osobistego pulpitu (osobistej maszyny wirtualnej)?
- W przypadku zbiorczego pulpitu, czy osoba żądająca połączenia ma rozłączoną sesję łączności z maszyną wirtualną?

Jeśli połączenie nie istnieje, żądanie jest przesyłane do serwera RD Virtualization Host, który zawiera najmniejszą liczbę aktywnych maszyn wirtualnych, przy czym serwer ten przygotowuje VM do połączenia.



Rysunek 1-3 RD Connection Broker pośredniczy również w połączeniach do maszyn wirtualnych na serwerach RD Virtualization Host.

RD Connection Broker zawiera tylko jedną formę mechanizmu równoważenia obciążeń – śledzenie liczby aktywnych sesji bądź uruchomionych maszyn wirtualnych – ale może zostać zintegrowany z rozwiązaniami równoważenia obciążeń innych firm, które wykorzystują bardziej zaawansowane kryteria, jak obciążenie pamięci i procesora, pora dnia lub wybrana aplikacja.

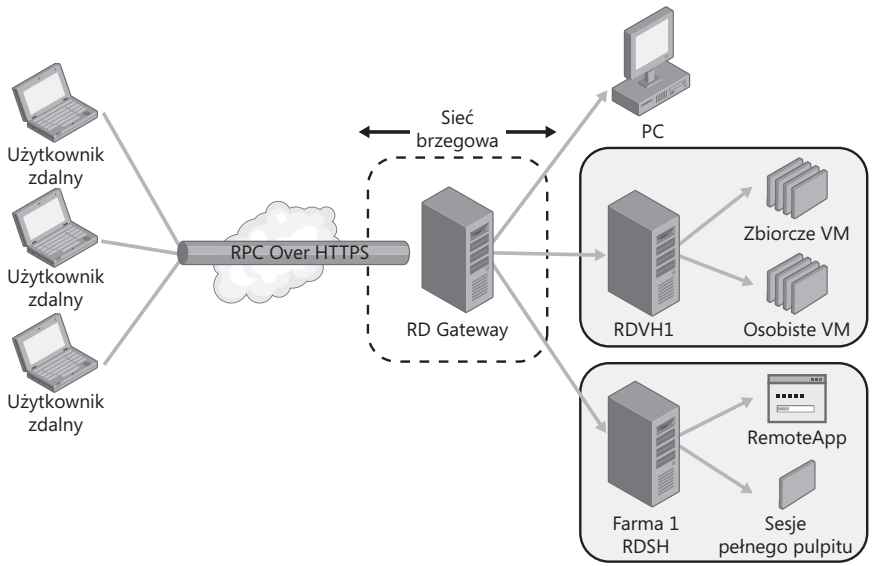
Rozdział 9 zawiera omówienie wykorzystania RD Connection Broker do obsługi farm serwerów RDSH oraz zbiorczych i osobistych maszyn wirtualnych.

RD Gateway

W mrocznych czasach przed pojawieniem się Windows Server 2008, jeśli chcieliśmy połączyć się z serwerem terminali gdzieś z zewnętrznego świata, korzystając tylko z tych narzędzi, które dostępne były wraz z systemem, konieczne było otwarcie na zaporze portu 3389 (domyślnego portu protokołu RDP), aby serwer terminali mógł zaakceptować przychodzące połączenia. Większość administratorów jednak wolała tego nie robić ze względu na dziurę w zabezpieczeniach, która otwierała się wraz z tym portem.

Jedną z usług roli RDS dostępnych w Windows Server 2008 R2 jest RD Gateway (Brama usług pulpitu zdalnego). Usługa ta umożliwia autoryzowanym użytkownikom zdalnym łączenie się z zasobami w wewnętrznej sieci korporacyjnej lub prywatnej z dowolnego urządzenia

podłączonego do Internetu, bez względu na to, czy urządzenie to jest oryginalnie częścią domeny, czy też np. komputerem publicznym. Jak widać na rysunku 1-4, zasoby sieciowe mogą obejmować serwery RDSH obsługujące pełne sesje pulpitu lub programy RemoteApp, maszyny wirtualne lub komputery z włączoną obsługą pulpitu zdalnego. Mówiąc inaczej, osoby uzyskujące dostęp do sieci korporacyjnej z Internetu mogą wykorzystać RDP w celu połączenia z pełnymi pulpitami, indywidualnymi aplikacjami, a nawet swoimi komputerami biurkowymi – zależy to tylko od tego, co skonfiguruje administrator.



Rysunek 1-4 RD Gateway zapewnia bezpieczny dostęp do sieci korporacyjnej z innej sieci, takiej jak Internet.

RD Gateway wykorzystuje protokół RDP over HTTPS do utworzenia bezpiecznego, szyfrowanego łącza pomiędzy komputerem zdalnym w Internecie i siecią wewnętrzną. Wymaga otwarcia tylko portu 443 (który zapewne i tak jest otwarty w celu zapewnienia bezpiecznej łączności internetowej). W ten sposób RD Gateway realizuje następujące działania:

- Pozwala użytkownikom zdalnym łączyć się z zasobami sieci wewnętrznej z Internetu przy użyciu szyfrowanego połączenia bez konieczności konfigurowania łączy VPN.
- Udostępnia zaawansowany model zabezpieczeń, który umożliwia kontrolę nad dostępem do określonych zasobów sieci wewnętrznej.
- Zapewnia bezpośrednie (*point-to-point*) połączenia RDP, które można ograniczyć, zamiast dawania użytkownikom zdalnym dostępu do wszystkich zasobów sieci wewnętrznej.
- Umożliwia większości użytkowników zdalnych dostęp do zasobów sieci wewnętrznej, zlokalizowanych za zaporą ogniową w sieci prywatnej lub za urządzeniami NAT. Przy użyciu RD Gateway nie ma potrzeby wykonywania dodatkowej konfiguracji serwera ani klientów (poza otwarciem portu 443 na zaporze).

Konsola RD Gateway Manager (Menedżer bramy usług pulpitu zdalnego) umożliwia skonfigurowanie zasad autoryzacji w celu zdefiniowania warunków, które muszą spełniać użytkownicy zdalni przed uzyskaniem połączenia do zasobów wewnętrznych. Przykładowo, można określić:

- Kto może łączyć się z RD Gateway (inaczej mówiąc, którzy użytkownicy bądź komputery mogą uzyskać połączenie).
- Jakie zasoby sieciowe (komputery lub grupy komputerów) są dostępne dla użytkowników.
- Czy dozwolone jest przekierowanie urządzeń i dysków.
- Czy klienci muszą korzystać uwierzytelniania przy użyciu kart inteligentnych, haseł, czy jednego z nich.

W celu dalszego podniesienia zabezpieczeń można skonfigurować serwery RD Gateway i klientów RDC do korzystania z mechanizmu Network Access Protection (NAP). Jest to mechanizm tworzenia zasad kondycji, wymuszania ich i naprawy (w razie potrzeby) dołączony w pakiecie Windows XP Service Pack 3 i standardowo obecny w Windows Vista, Windows Server 2008, Windows 7 i Windows Server 2008 R2. Przy użyciu NAP administratorzy systemów mogą wymusić spełnienie warunków kondycji przez komputery klienckie, takie jak instalacja wymaganych poprawek zabezpieczeń, określona konfiguracja komputera bądź instalacja wymaganego oprogramowania przed dopuszczeniem połączenia z serwerem RD Gateway.

Serwery RD Gateway mogą być również wykorzystywane w połączeniu z Microsoft Internet Security and Acceleration (ISA) albo Forefront Threat Management Gateway (TMG) w celu podniesienia zabezpieczeń. W tym scenariuszu serwery RD Gateway lokalizowane są w sieci prywatnej, a nie brzegowej, w której znajdują się hosty ISA lub TMG. Połączenie SSL pomiędzy klientem RDC a serwerem ISA lub TMG kończy się na serwerze dostępnym z Internetu.

Konsola RD Gateway Manager udostępnia narzędzia pozwalające na monitorowanie bieżącego statusu połączeń, kondycji klientów i zdarzeń. Przy użyciu tej konsoli można określić zdarzenia (takie jak zakończone niepowodzeniem próby dostępu do serwera), które będziemy chcieli monitorować.

RD Gateway może współpracować z plikami RDP przechowywanymi na komputerach klienckich, z RD Web Access lub z mechanizmem RemoteApp and Desktop Connections. W tych ostatnich przypadkach można skonfigurować zdalną przestrzeń roboczą, która udostępni witrynę zawierającą odpowiednie łącza do aplikacji i zagwarantuje, że osoba lub komputer wykorzystywany do połączenia spełnia warunki określone w regułach RD Gateway.

RD Gateway wykorzystuje bardzo niewiele zasobów i przy odpowiedniej konfiguracji może obsłużyć setki przychodzących połączeń, zatem może być śmiało łączony z innymi rolami, które też powinny znaleźć się w sieci brzegowej.

RD Licensing

Usługa roli RD Licensing (Licencjonowanie usług pulpitu zdalnego) jest odpowiedzialna za śledzenie, kto ma licencję na korzystanie z serwerów RDSH. Nie kto jest *autoryzowany* do tego – za to odpowiadają prawa użytkownika AD DS lub ustawienia RD Gateway, zależnie od tego, na którym poziomie administrator określi uprawnienia. RD Licensing jest

systemem zarządzania licencjami, który pozwala serwerom RDSH uzyskiwać i zarządzać klienckimi licencjami dostępowymi (RDS CAL) dla urządzeń i użytkowników, którzy łączą się z serwerami.

> **Uwaga** RD Licensing wspiera wcześniejsze wersje serwerów terminali aż do Windows 2000 Server. Ponadto system operacyjny wspiera do dwóch równoległych połączeń w celu zdalnej administracji komputerem i dla tych połączeń nie są potrzebne licencje dostępowe ani serwer licencji.

Serwery RDSH mogą zostać skonfigurowane, aby wymagały albo licencji dla użytkownika, albo dla urządzenia. Więcej informacji na temat RD Licensing zawiera rozdział 12, „Licencjonowanie usług pulpitu zdalnego", jednak podstawowe zasady są następujące: każdy serwer hosta sesji ustala, czy łączący się użytkownik lub komputer dysponuje ważną licencją. Jeśli tak (i gdy użytkownik ma uprawnienia wymagane do logowania), serwer zezwala na połączenie. W przeciwnym razie RDSH próbuje połączyć się z serwerem licencji, aby ustalić, czy jest dostępna licencja dla tego urządzenia lub użytkownika. Serwer licencji wówczas albo alokuje licencję dla urządzenia, albo modyfikuje właściwości konta użytkownika w AD DS, sygnalizując użycie licencji. Jeśli serwer hosta sesji nie może połączyć się z serwerem RD Licensing, wystawi tymczasową licencję, o ile trwa jeszcze okres przejściowy, wynoszący 120 dni od momentu instalacji roli.

Serwery obsługujące rolę RD Licensing utrzymują bazę danych, która rejestruje wystawianie RDS CAL. W przypadku licencji na urządzenie są one przypisywane do komputerów. W przypadku licencji na użytkownika licencja nie jest faktycznie przypisywana, ale jej użycie jest rejestrowane w AD DS i można je śledzić.

RD Licensing jest usługą powodującą bardzo małe obciążenie komputera, wymagającą bardzo niewielkiego czasu procesora i pamięci w normalnym działaniu. Zużycie pamięci jest mniejsze niż 10 MB. Również obciążenie nakładane na dysk jest minimalne, nawet dla znaczącej liczby klientów: baza danych powiększa się o 5 MB na każde 6000 wydanych licencji. Serwer licencji jest aktywny tylko na żądanie przychodzące z serwera RDSH i jego wpływ na ogólną sprawność komputera jest bardzo mały. Z tego względu w większości wypadków usługa RD Licensing może być instalowana razem z usługą RDSH. Jedynie w największych wdrożeniach rola ta powinna być rozmieszczana na oddzielnym komputerze.

Jakkolwiek tylko dostęp do roli RDSH wyzwala rejestrowanie użycia RDS CAL, korzystanie z dowolnej części infrastruktury RDS wymaga RDS CAL (zaś w przypadku wdrożeń wykorzystujących tylko wirtualne pulpity VDI CAL).

Jak inne usługi współpracują z RDS

Rola RDS nie funkcjonuje w próżni. Wiele innych ról pomaga w obsłudze różnych usług związanych z RDS i bez nich całe rozwiązanie nie mogłoby działać. Oprócz zasadniczych usług roli RDS i ich wzajemnych powiązań, trzeba rozumieć również ich zależność od innych ról Windows Server. W tym rozdziale zajmiemy się przedstawieniem tych ról i tego, jak wspierają one funkcjonalność RDS.

Jakie są te role i jak pasują do siebie? Jak wpasowują się w inne, niezwiązane z RDS części infrastruktury, takie jak Hyper-V, IIS, certyfikaty czy Active Directory, aby wymienić tylko najważniejsze?

Połączenie klienckie

Tak, to być może jest oczywiste, ale warto zwrócić na to uwagę: sposób interakcji klienta z usługami roli RDS określa, jakie będą wrażenia użytkownika uzyskiwane z określonego punktu końcowego.

Niezależnie od tego, czy tym punktem końcowym jest sesja na serwerze RDSH, maszyna wirtualna utrzymywana na RD Virtualization Host, czy wręcz fizyczny komputer, fundamentalna zależność pomiędzy klientem i punktem końcowym składa się z trzech części: programu klienta RDC, łącza RDP i samego punktu końcowego.

- Komponent RDC inicjuje połączenie do punktu końcowego i odbiera dane wysyłane przez serwer.
- Komponent serwerowy w punkcie końcowym współdziała z samym systemem operacyjnym i odbiera otrzymywane informacje (na przykład wytwarzane dźwięki czy wyświetlane bitmapy), konwertuje je na polecenia RDP i serializuje je w celu przesłania do klienta.
- Protokół zapewnia połączenie pomiędzy klientem i punktem końcowym; to on definiuje rodzaj informacji, które są przekazywane pomiędzy nimi poprzez wirtualne kanały.

> **Uwaga** Skąd bierze się rozróżnienie pomiędzy RDP a RDC? RDP to Remote Desktop Protocol, czyli protokół używany do przesyłania danych wejściowych od użytkownika i danych wyjściowych z aplikacji pomiędzy klientem a serwerem. RDC to Remote Desktop Connection, program kliencki, który inicjuje i zarządza połączeniem RDP.

Mówiąc w skrócie, klient żąda połączenia, punkt końcowy formatuje wywołania do aplikacji lub systemu operacyjnego w taki sposób, który klient (lub serwer, zależnie od tego, w którą stronę informacja jest przesyłana w danej transakcji) może zrozumieć, zaś RDP przekazuje odpowiednie informacje, pozwalające użytkownikowi komunikować się z aplikacjami na serwerze, tak jakby były uruchomione lokalnie.

Ta komunikacja opiera się na *wirtualnych kanałach*, dwukierunkowych strumieniach połączenia udostępnianych przez RDP. Tworzą one potok danych pomiędzy klientem RDC i punktem końcowym, przekazując określone typy informacji, takie jak obrazy i tekst, naciśnięcia klawiszy czy ruch myszy. Kanały wirtualne stanową sposób rozszerzenia funkcjonalności RDP, która jest dostępna od czasów Windows 2000 Server i są również wykorzystywane przez niektóre funkcje RDS, takie jak przekierowanie urządzeń i dźwięku.

Wiele jednak zmieniło się od czasów Windows 2000 Server, a jednym z komponentów, który zmienił się zasadniczo, jest statyczny zbiór 32 wirtualnych kanałów, oryginalnie dostępny w RDP 5.1 – ta liczba nie jest już wystarczająca. Obecnie dostępnych jest znacznie więcej rodzajów danych i oczywiste jest, że pojawiać się będą nowe, dziś jeszcze nieznane. Dodatkowo statyczne kanały wirtualne miały znaczące ograniczenie: były tworzone na początku połączenia i zamykane na zakończenie. Jeśli w trakcie sesji chcieliśmy dołączyć

nowe urządzenie, nie mogło ono użyć kanałów wirtualnych, o ile nie zamknęliśmy połączenia i nie wznowiliśmy go ponownie.

> **Ważne** Zamknięcie połączenia powoduje jego zakończenie po stronie serwera. Rozłączona (zerwana) sesja nadal istnieje na serwerze i użytkownik może się ponownie z nią połączyć.

Z tego względu w RDS wprowadzono *dynamiczne kanały wirtualne*, czyli takie, które klient tworzy na żądanie i zamyka, gdy już nie są potrzebne, w trakcie trwania sesji. Jeśli ktoś jest zainteresowany interfejsami, które pozwalają tworzyć dynamiczne kanały wirtualne (albo po prostu tym, jak one działają), polecamy lekturę dokumentu PDF „Functionality for RDS Scripters and Developers" zamieszczonego na dołączonym dysku CD[5].

Hostowanie maszyn wirtualnych

Przez pewien czas możliwe było wirtualizowanie ról Terminal Services, ale Hyper-V nie był wymaganym komponentem wdrożenia. W przypadku RDS Hyper-V jest niezbędny, jeśli chcemy korzystać z funkcji udostępniania maszyn wirtualnych.

Rola Hyper-V jest instalowana automatycznie po wybraniu usługi roli RD Virtualization Host. Ponieważ rola ta jest zależna od Hyper-V, jest to jedyna usługa roli RDS, której nie można zwirtualizować.

Uwierzytelnianie serwerów przy użyciu certyfikatów

Jakkolwiek nie jest konieczne korzystanie z serwera Certificate Authority (CA), aby móc korzystać z RDS, bez wątpienia konieczne będą certyfikaty pochodzące z jakiegoś źródła (być może zewnętrznego).

Jednym z ciekawszych zagadnień dotyczących RDS jest wymaganie zaufania pomiędzy klientem i serwerem. Co oczywiste, serwer musi ufać klientowi, gdyż jest potencjalną furtką do sieci korporacyjnej. Jednak klient również musi ufać serwerowi. Klient przekazuje nazwę użytkownika i hasło, obowiązujące w sieci firmowej, zatem ważne jest, aby serwer, z którym łączy się klient, był właściwym punktem końcowym, a nie sfałszowanym serwerem, służącym wyłudzaniu poświadczeń.

W celu zagwarantowania tożsamości punktu końcowego można na serwerze i kliencie zainstalować odpowiedni certyfikat. W tym celu należy uzyskać certyfikat z własnego (firmowego) rozwiązania PKI albo zakupić go od publicznego urzędu certyfikacji.

> **Ważne** Wszystkie serwery RDSH w jednej farmie muszą używać tego samego certyfikatu do uwierzytelniania opartego na certyfikatach.

Certyfikaty są również używane do:

- Uwierzytelniania tożsamości serwera RD Gateway i umożliwienia mu tworzenia bezpiecznego kanału do klienta.

5 Ze względu na ograniczenia praw autorskich dokument ten, podobnie jak cała pozostała zawartość dysku CD dołączonego do książki, dostępny jest tylko w języku angielskim.

- Podpisywania plików RDP.
- Zapewniania dostępu poprzez protokół HTTPS do witryny RD Web Access.

Włączanie dostępu do sieci rozległej i wyświetlanie zasobów zdalnych

Dwa komponenty RDS wymagają IIS: RD Web Access oraz RD Gateway. Wymaganie obecności IIS dla RD Web Access jest oczywiste: udostępnia on informacje o programach RemoteApp i pulpitach poprzez dwa adresy URL. Jeden z nich wyświetla witrynę RD Web Access, zaś drugi zapewnia wsparcie dla mechanizmu RemoteApp and Desktop Connections.

IIS jest również wymagany do działania RD Gateway, gdyż ten ostatni kapsułkuje ruch RDP w protokół HTTPS, zatem potrzebuje określonych komponentów IIS.

IIS jest instalowany automatycznie po wybraniu usług roli RDS, które go wymagają.

Aktualizowanie ustawień użytkowników i komputerów

Wybór usługi katalogowej Active Directory (AD DS) jako roli wspomagającej jest tak oczywistym wyborem, że można o tym po prostu nawet nie myśleć, jednak jest to krytyczny element funkcjonowania scentralizowanej infrastruktury przetwarzania – także pod takimi względami, których ktoś mógłby nie oczekiwać. AD DS zarządza:

- Zasadami grupy, które pozwalają konfigurować serwery RDSH oraz uruchamiane na nich sesje użytkowników.
- Tym, czy użytkownik ma, czy też nie ma praw do łączenia się z serwerem RDSH.
- Przetwarzaniem licencji na użytkownika, jeśli korzysta się z tego modelu licencjonowania.

Funkcjonalność dla twórców skryptów i programistów

Bardzo ważną rzeczą jest zrozumienie, że RDS nie jest po prostu produktem – choć jest nim bez wątpienia – ale także platformą projektową, zarówno dla niezależnych dostawców oprogramowania, jak i dla konsultantów budujących niestandardowe rozwiązania. Windows Server 2008 zawiera bardzo wiele nowych interfejsów API, zaś w Windows Server 2008 R2 pojawiło się jeszcze kilka. Choć omówienie sposobów wykorzystania tych interfejsów wykracza poza tematykę tej książki, informacje zamieszczone na dołączonej płycie CD przedstawiają niektóre rozszerzenia dostępne dla programistów poprzez publiczne interfejsy.

Na dołączonym nośniku Szczegółowe omówienie RDS API zawiera dokument „Functionality for RS Scripters and Developers" na dołączonej do książki płycie CD. Szersze i bardziej szczegółowe omówienie wykorzystania tych API znaleźć można w MSDN.

Uwaga Publiczne interfejsy (nazywane też API, czyli Application Programming Interface) są interfejsami, które (no właśnie) są dostępne publicznie i udokumentowane w MSDN, dzięki czemu programiści mogą z nich korzystać. Interfejsy prywatne nie są udokumentowane. Główna różnica to zapewnienie wsparcia. Interfejs prywatny może ulec zmianie (pod względem funkcjonalności, formatu danych czy wręcz obecności) w dowolnym momencie, jeśli będzie to potrzebne ludziom, którzy go stworzyli (w tym wypadku programistom firmy Microsoft). Żadne API nie zostanie zmienione bez wcześniejszej zapowiedzi. Nawet jeśli istnieje możliwość zbudowania rozwiązania wykorzystującego interfejs prywatny, znacznie lepszym pomysłem będzie oparcie go na interfejsie publicznym, po prostu w celu uniknięcia potencjalnych problemów.

Podsumowanie

W rozdziale tym przedstawiliśmy ogólny zarys cech i funkcjonalności Usług pulpitu zdalnego (RDS) w systemie Windows Server 2008 R2. W tym momencie Czytelnik powinien już wiedzieć:

- Jak ta rola rozwijała się od momentu, gdy stała się częścią Windows 10 lat temu.
- Do czego służy RDS.
- Nowe przypadki biznesowe, które wspiera RDS w systemie Windows Server 2008 R2.
- Jak inne role Windows (i klient) wspierają funkcjonalność RDS.

W rozdziale 2 pokażemy związki pomiędzy ogólną architekturą Windows i RDS.

Dodatkowe zasoby

W wymienionych źródłach można znaleźć dodatkowe informacje i narzędzia dotyczące tego rozdziału:

- Więcej informacji na temat fundamentalnych koncepcji systemu operacyjnego, które mają wpływ na funkcjonalność RDSH i RD Virtualization Host (i ich wymiarowanie) zawiera rozdział 2, „Kluczowe koncepcje architektury RDS".
- Informacje na temat instalowania i konfigurowania serwera RDSH zawiera rozdział 3, „Wdrażanie pojedynczego serwera RDSH".
- Wskazówki dotyczące konfigurowania serwera RD Virtualization Host w celu obsługi zbiorczych i osobistych pulpitów (maszyn wirtualnych) zawiera rozdział 4, „Wdrażanie pojedynczego serwera RD Virtualization Host".
- Konfigurowanie profili użytkowników na potrzeby RDS omówione jest w rozdziale 5, „Zarządzanie danymi użytkowników we wdrożeniu RDS".
- Zagadnienia integracji systemów klienckich i serwera dla potrzeb wyświetlania, drukowania oraz przekierowania dźwięku i urządzeń omówione są w rozdziale 6, „Konfigurowanie środowiska użytkowników".

- Aby dowiedzieć się, jak zablokować zmiany środowiska użytkownika przy użyciu zasad grupy, należy przeczytać rozdział 7, „Formowanie i zabezpieczanie środowiska użytkownika”.
- Informacje o zabezpieczaniu połączeń RDP w sieciach lokalnych zawiera rozdział 8, „Zabezpieczanie połączeń RDP”.
- Omówienie wykorzystania RD Connection Broker do wdrożenia farmy serwerów RDSH lub puli maszyn wirtualnych zawiera rozdział 9, „Wdrożenia wieloserwerowe”.
- Publikowanie zasobów za pośrednictwem rozwiązań RD Web Access oraz RemoteApp and Desktop Connections jest omówione w rozdziale 10, „Zapewnianie dostępności RDS z Internetu”.
- Problematyka zarządzania sesjami na serwerach hosta sesji stanowi treść rozdziału 11, „Zarządzanie sesjami pulpitu zdalnego”.
- Informacje na temat licencjonowania usług pulpitu zdalnego i wykorzystania serwera RD License zawiera rozdział 12, „Licencjonowanie usług pulpitu zdalnego”.
- Więcej informacji na temat interfejsów publicznych (API) dostępnych dla programistów zawiera RDS Reference pod adresem *http://msdn.microsoft.com/en-us/library/aa383494(VS.85).aspx*, zaś pogłębioną dokumentację i przykłady kodu źródłowego można znaleźć w RDS Code Gallery pod adresem *http://code.msdn.microsoft.com/rdsdev*.

ROZDZIAŁ 2

Kluczowe koncepcje architektury RDS

Przed przystąpieniem do instalowania usług roli RDS konieczne jest rozważenie kilku zagadnień zarówno technicznych, jak i biznesowych. Rozdział ten ma na celu odpowiedzieć na pojawiające się pytania, ukazując zarówno szczegóły architektury systemowej, które są szczególnie istotne dla obu modeli dostarczania aplikacji wspieranych przez RDS, jak i decyzje biznesowe, które trzeba podjąć przed implementacją rozwiązania. Pozwoli to na lepsze zaplanowanie zasobów niezbędnych do realizacji potrzeb. W tym rozdziale przedstawimy takie zagadnienia, jak:

- Wewnętrzne struktury systemu Windows Server 2008 R2, szczególnie istotne dla wymiarowania ról RDS.
- Sposoby dobierania wielkości serwerów RD Session Host (RDSH) i RD Virtualization Host (RDVH).
- Wymagania po stronie klienta, dotyczące nowych funkcji RDS.
- Charakterystyka aplikacji, które będą poprawnie działać na serwerach RDSH.
- Decyzje techniczne wynikające z potrzeb biznesowych, takie jak tryb licencjonowania lub rodzaje sprzętu klienckiego, najbardziej właściwe dla konkretnego przedsiębiorstwa.

Uwaga Część tego rozdziału poświęcona jest zagadnieniom skalowania wydajności na istniejącym serwerze terminali. Podczas ustalania kolejności rozdziałów tej książki zdecydowaliśmy umieścić planowanie przed instalowaniem. Szczegóły procesu instalacyjnego zawiera rozdział 3, „Wdrażanie pojedynczego serwera RD Session Host" oraz rozdział 4, „Wdrażanie pojedynczego serwera RD Virtualization Host".

Poznawanie systemu dostarczania aplikacji

Zanim zagłębimy się w problemy dotyczące architektury pamięci czy wskazówki dotyczące wymiarowania serwera, musimy wiedzieć, co w istocie robią serwery RDSH i RDVH. Zrozumienie, jak działa każda z platform dostarczania aplikacji, jest podstawowym warunkiem zrozumienia wskazówek i sposobów wymiarowania.

Serwery RD Session Host

Komputer odgrywający rolę hosta sesji usług pulpitu zdalnego jest w istocie współużytkowaną stacją roboczą dla wielu równocześnie pracujących użytkowników. Gdy jest używany, serwer uruchamia żądane aplikacje i ładuje pliki do pamięci. Zapisuje też pliki użytkowników. Gdy użytkownik loguje się do serwera RDSH, system serwera ładuje profil użytkownika, dzięki czemu otrzymuje on dostosowane, dobrze znane środowisko pracy. Serwer wykonuje więc to wszystko, co robi zwykła stacja robocza... ale robi to dla wielu użytkowników jednocześnie. W praktyce oznacza to, że serwer hosta sesji usług pulpitu zdalnego musi:

- Próbować rozdzielać wykorzystanie czasu procesora pomiędzy wszystkie sesje w taki sposób, aby jedna z nich nie zużyła wszystkich cykli zegara kosztem innych sesji.
- Obsługiwać nowych użytkowników, gdy się logują, nadal pozwalając na pracę bieżących użytkowników.
- Uruchamiać wiele wystąpień (instancji) tych samych aplikacji w tak efektywny sposób, jak to tylko możliwe.
- Kontrolować dostępną pamięć fizyczną i wykorzystywać ją możliwie oszczędnie, aby zapewnić wydajną pracę wszystkich użytkowników.
- Izolować sesje od siebie nawzajem, aby różni uruchamiający te same aplikacje na tym samym komputerze nie widzieli danych innych użytkowników.

Serwery RDVH

Model dostarczania aplikacji wykorzystywany przez serwery RDVH wygląda nieco inaczej. Serwer taki nie jest współużytkowaną stacją roboczą; jest platformą, na której działa zbiór indywidualnych stacji roboczych (maszyn wirtualnych, VM), z których każda ma własne środowisko operacyjne. Maszyny wirtualne są w pełni odizolowane od siebie nawzajem. Mogą pracować pod kontrolą różnych systemów operacyjnych, używać niekompatybilnych sterowników urządzeń, wykonywać aplikacje wymagające wielkich zasobów i nawet ich awaria nie ma wpływu na inne VM uruchomione na tym samym hoście. Dopóki działanie samego systemu RDVH nie zostanie zakłócone, poszczególne maszyny wirtualne nie mają wpływu na siebie nawzajem.

Podczas konfigurowania VM (szczegółowe omówienie znajduje się w rozdziale 4) trzeba określić, jaką wielkość pamięci i ile procesorów otrzyma każda z nich. Niewykorzystywana pamięć lub moc procesora nie jest rozdzielana pomiędzy pozostałe maszyny wirtualne na tym samym hoście. Oznacza to, że potrzebne jest dobre wyobrażenie, jakie będą potrzeby każdej VM i jaki sprzęt będzie potrzebny do ich obsłużenia.

Każdy z tych modeli dostarczania aplikacji działa inaczej, ale zasadniczo realizują one ten sam cel: pozwalają większej liczbie osób korzystać z tego samego sprzętu w tym samym czasie. Obydwa wymagają nieco żonglerki po stronie systemu operacyjnego. Nasze zadanie to zapewnienie każdemu rodzajowi serwera dostatecznych zasobów, aby żonglerka ta przebiegała możliwie sprawnie i wydajnie. Aby to osiągnąć, musimy wiedzieć, jak serwery RDSH wykonują wszystkie te zadania.

Powiązane cechy Windows Server 2008 R2

W tym podrozdziale przedstawimy zasady działania niektórych komponentów systemowych, które mają największy wpływ na funkcjonowanie RDS i pozwolą zrozumieć, jak serwery RDSH lub RDVH alokują zasoby dla obsługiwanych użytkowników. W szczególności zajmiemy się takimi zagadnieniami, jak:

- Jakie znaczenie dla roli RDS ma fakt, że Windows Server 2008 R2 dostępny jest tylko w wersji 64-bitowej.
- Jak działają maszyny wirtualne.
- Jak serwery dostarczające aplikacje alokują cykle procesora dla wszystkich użytkowników.
- Jak serwery wykonują zarządzanie pamięcią dla sesji i maszyn wirtualnych.

Kolejne części dotyczą głównie serwerów RDSH, gdyż działanie ich najbardziej różni się od tego, co znamy z jednostanowiskowych systemów. Choć hosty maszyn wirtualnych również muszą rozdzielać zasoby pomiędzy poszczególne VM, same maszyny wirtualne bardziej przypominają zwykły system dla pojedynczego użytkownika.

Windows Server 2008 R2 istnieje tylko w wersji 64-bitowej

Jedną z najbardziej podstawowych rzeczy, które musimy zrozumieć, jest fakt, że Windows Server 2008 R2 jest systemem 64-bitowym i nie istnieje inna jego wersja. Windows 7, podobnie jak Windows Vista, istnieją zarówno w odmianie 32-, jaki 64-bitowej, ale w przypadku serwera opcja 32-bitowa już nie jest dostępna. Windows Server 2008 był ostatnią 32-bitową platformą serwerową firmy Microsoft.

> **Uwaga** Wcześniejsze wydanie tej książki, dotyczące Windows Server 2008, zawierało omówienie mechanizmów Physical Address Extensions (PAE) oraz Addres Windowing Extensions (AWE), które w systemie 32-bitowym pozwalały wykroczyć poza granicę przestrzeni adresowej wynoszącą 4 GB. Jednak żaden z tych mechanizmów nie jest wspierany – ani też potrzebny – w 64-bitowym systemie, toteż nie zostały uwzględnione w tej książce.

Z punktu widzenia potrzeb serwerów hosta sesji pulpitu zdalnego, przejście na platformę 64-bitową jest niemal całkowicie dobrą rzeczą (za chwilę wyjaśnimy, co robi tu słowo „niemal"). W 32-bitowych systemach operacyjnych największym ograniczeniem i wąskim gardłem serwerów terminali była pamięć, choć prędkość działania dysków zajmowała bliskie

drugie miejsce. 32-bitowy system nie może adresować więcej niż 4 GB pamięci wirtualnej, bez względu na to, ile pamięci fizycznej zainstalujemy w komputerze. W wersji Standard systemy Windows Server nie obsługiwały nawet instalacji większej pamięci niż 4 GB, zatem nie można było sięgnąć po rozwiązania zastępcze, takie jak PAE lub AWE, umożliwiające systemowi operacyjnemu przechowywać i odwoływać się do danych w pamięci większej niż 4 GB, nawet jeśli nie był w stanie „zobaczyć" jej całej w jednym momencie. Obecnie 64-bitowe wersje Windows widzą do 2^{44} adresów pamięci wirtualnej (16 TB), co oznacza w praktyce, że mogą one użyć tyle pamięci, ile potrzebujemy (albo ile uda się włożyć do serwera), bez potrzeby stosowania żadnych trików, których wymagały systemy 32-bitowe.

Powodem, dla którego przy ocenie 64-bitowej wersji pojawił się zwrot „niemal całkowicie dobrą", jest problem z obsługą starszych sterowników urządzeń i aplikacji. Jak można się przekonać, 32-bitowe aplikacje zazwyczaj działają w 64-bitowym systemie bez zakłóceń. W większości wypadków program, który działał z powodzeniem na 32-bitowym serwerze terminali, będzie też działał na 64-bitowym RDSH. Jednak 64-bitowy system wymaga 64-bitowych sterowników. Na przykład starsze drukarki, które chcielibyśmy nadal wykorzystywać i obsługiwać, mogą nie mieć 64-bitowych sterowników.

Tym niemniej nawet oporne sterowniki drukarek nie muszą zburzyć naszych planów scentralizowania dostarczania aplikacji. Po pierwsze, jeśli możemy użyć mechanizmu Easy Print (omówionego w rozdziale 6, „Konfigurowanie środowiska użytkowników") dla naszych drukarek, nie będziemy musieli instalować ich sterowników na serwerach RDSH, ale po prostu użyjemy sterowników zainstalowanych na komputerach klienckich. Jeśli zaś Easy Print nie jest opcją, którą moglibyśmy wykorzystać, możemy wykorzystać RDVH, aby obsłużyć tych użytkowników, którzy muszą korzystać ze starszych urządzeń drukujących.

W przypadku wirtualizacji, 64-bitowy system jest prawdziwym sukcesem – z tego też powodu Hyper-V zawsze był 64-bitowy. Systemy gości (maszyn wirtualnych) nie muszą mieć systemów 64-bitowych, zatem tu nie pojawią się problemy dotyczące aplikacji lub sterowników, o ile tylko środowisko użytkownika będzie oparte na Windows XP SP2 lub wersji późniejszej. W tym wypadku 64-bitowy system hosta oznacza po prostu, że możemy zainstalować tyle pamięci, ile potrzebują wszystkie maszyny wirtualne.

Oszczędna gospodarka cyklami procesora

W komputerze nic nie wydarza się bez udziału procesora. Gdy serwer obsługuje dziesiątki użytkowników, pojawia się silna konkurencja o dostępne cykle procesora. W tej części zajmiemy się tym, w jaki sposób serwer RDSH decyduje, kto powinien uzyskać przydział czasu procesora.

Użytkownicy uruchamiają aplikacje, ale system operacyjny nie zna takiego pojęcia. System zajmuje się procesami i wątkami, które realizują wykonywanie aplikacji. *Proces* definiuje robocze środowisko aplikacji, w tym jego priorytet pod względem przydzielania czasu procesora, nazwę obrazu aplikacji związaną z tym procesem (na przykład Winword.exe), identyfikator procesu (process ID – PID), którego używa system do unikatowego oznakowania procesu, obszary pamięci przydzielone do procesu, łącze do procesu nadrzędnego, który go uruchomił, oraz dowolne inne informacje, które aplikacja musi znać, aby działać i współpracować z innymi uruchomionymi aplikacjami.

Wprost ze źródła

Jak 64-bitowe Windows radzą sobie jako serwer RDSH?

Jeff Heatton
Operations Engineer, Microsoft

W ciągu ostatnich miesięcy wiele z naszych serwerów zostało zaktualizowanych do wersji 64-bitowej. Mogliśmy więc zobaczyć, że ten sam fizyczny serwer, który dawał sobie radę z powiedzmy 55 użytkownikami, pracując pod kontrolą 32-bitowego systemu z 4 GB pamięci RAM, teraz obsługuje 150 użytkowników bez widocznego wysiłku w trybie 64-bitowym z pamięcią rozszerzoną do 8 GB. 64-bitowe środowisko wydaje się działać wręcz doskonale i przypuszczam, że możemy łatwo dokonać dalszej rozbudowy, jedynie dodając więcej pamięci poszczególnym serwerom. Na niektórych serwerach zarejestrowaliśmy nawet więcej niż 300 równoległych sesji bez żadnych problemów wydajnościowych.

Zauważyliśmy natomiast, że w naszym zastosowaniu obciążenie generowane przez tę samą aplikację jest silnie zależne od regionu, gdyż użytkownicy mają odmienne wzorce pracy. Europejczycy generują znacznie większy ruch, podczas gdy ludzie ze Stanów Zjednoczonych i Azji pozwalają farmom RDS na lekkie wytchnienie.

Jak to działa

Dlaczego proces musi mieć zarówno nazwę, jak i PID

Ktoś mógłby spytać, czemu służy podwójna identyfikacja procesu, czyli po co ma on nazwę obrazu (będącą też nazwą pliku wykonywalnego) i oprócz tego PID? Odpowiedź jest prosta – nazwy obrazów nie muszą być unikatowe, szczególnie w przypadku RDSH jest wysoce prawdopodobne, że w jednej chwili uruchomiona może być więcej niż jedna instancja tej samej aplikacji, a w każdym przypadku można zagwarantować istnienie więcej niż jednej instancji niektórych procesów systemowych (rozdział 3 zawiera informacje na temat procesów wspólnych dla wszystkich sesji).

Ponieważ także w granicach jednej sesji może wystąpić więcej niż jedna instancja, nie możemy identyfikować procesów przy użyciu nazw sesji. W momencie uruchamiania nowego procesu komponent systemu zwany menedżerem procesów nadaje mu unikatowy numer PID. Administratorzy usług pulpitu zdalnego często muszą odwoływać się do konkretnych numerów PID przy korzystaniu z narzędzia Remote Desktop Manager lub narzędzi wiersza polecenia, co zostało omówione w rozdziale 11, „Zarządzanie sesjami pulpitu zdalnego".

Procesy same jednak nie robią nic. Zamiast tego definiują one środowisko wykonawcze i zależności, które poszczególne części wykonywalne, zwane *wątkami*, muszą znać. Wątek musi wiedzieć, do jakiego procesu należy, kontekst zabezpieczeń, a dokładniej *żeton dostępu* (rekord informacji o przynależnych prawach, wynikających z tożsamości konta, która uruchomiła proces) oraz *informacje personifikacji* (czyli użyte poświadczenia zabezpieczeń). Muszą

one również śledzić swoje własne żądania wejścia/wyjścia (I/O). Podobnie jak procesy, wątki również mają określony priorytet. Ogólny poziom (zakres) tego priorytetu jest dziedziczony z procesu, ale wątek może skorygować swój własny priorytet w granicach tego zakresu.

Priorytet jest kluczową właściwością procesu lub wątku, gdyż określa on, jak często wątek uzyska przydział cykli procesora. Jak można się domyśleć, im wyższy priorytet, tym częściej wątek uzyskuje czas procesora. A ponieważ nic nie dzieje się bez udziału czasu procesora w celu wykonywania instrukcji, cecha ta jest krytyczna.

> **Uwaga** Jeśli ktoś chciałby zobaczyć, jak priorytet określonego procesu ma się do innych typów procesów, może wykorzystać narzędzie *Task Manager* (Menedżer zadań) i włączyć wyświetlanie kolumny *Base Priority* (Priorytet podstawowy). Łatwo zauważyć, że procesy systemowe, takie jak Csrss.exe (Win32 Subsystem) mają wyższy priorytet niż aplikacje użytkownika, zatem częściej uzyskują przydział czasu procesora. Jest to działanie zamierzone – na nic zdałaby się nawet największa responsywność aplikacji, jeśli same Windows przestaną odpowiadać.

Jedną z rzeczy, które odróżniają serwery RDSHs od innych typów serwerów, jest sposób wykorzystania priorytetyzowania procesów. Inne typy serwerów, najogólniej mówiąc, są projektowane tak, aby robiły tylko jedną rzecz, ale bardzo dobrze: przeszukują bazy danych, zarządzają pocztą elektroniczną lub udostępniają witryny internetowe. Ich priorytety są jasne: aplikacja pierwszego planu jest tą, która musi działać sprawnie i bez zakłóceń. Z tego względu procesy i wątki należące do takiej aplikacji mają wyższy priorytet, niż te w tle.

> **Uwaga** Samo to, że aplikacja pierwszego planu jest główną obsługiwaną, nie oznacza, że jej procesy mają *najwyższy* priorytet. Dogłębne omówienie zagadnień związanych z względnymi priorytetami różnych typów procesów znaleźć można w książce *Microsoft Windows Internals, Fifth Edition* Marka E. Russinovicha i Davida A. Solomona (Microsoft Press, 2009).

W odróżnieniu od innych serwerów, RDSH nie ma jednego jasnego celu czy też priorytetu (w odróżnieniu np. do serwera Exchange, który koncentruje się na jednym zadaniu: „*Muszę przesłać tę całą pocztę!*"). Miewają dziesiątki równoczesnych użytkowników, z których każdy robi co innego, ale wszyscy oczekują sprawnie reagującego środowiska. Z powodu konfliktu pomiędzy priorytetami poszczególnych użytkowników jedyną metodą działania serwera z zainstalowaną rolą RDSH jest ustawienie równego priorytetu wszystkich procesów i wątków użytkowników. Wyrównanie priorytetów procesów sprawia, że możemy oszacować obciążenie, jakiemu może podołać serwer, ustalając, jak wiele czasu procesora wymaga pojedyncza sesja użytkownika. Pokażemy, *jak* to zrobić przy użyciu narzędzia *Performance Monitor* w dalszej części tego rozdziału. Jednak kluczową rzeczą, którą musimy zapamiętać, jest fakt, że działanie polegające na zainstalowaniu roli RDSH optymalizuje system operacyjny do pełnienia tej roli w sieci. Serwer taki nie priorytetyzuje procesów tak, jak robi to serwer bazy danych lub poczty, gdyż potrzeby są zasadniczo odmienne.

Gdyby w jednej sesji została uruchomiona znaczna liczba wymagających aplikacji, mogłoby to potencjalnie wpłynąć na inne sesje, pomimo tego nawet, że wszystkie aplikacje mają ten sam priorytet. W systemie Windows Server 2008 problem ten był rozwiązywany

za pośrednictwem Windows System Resource Manager (WSRM), który obniżał priorytet wątku, jeśli wątki innych użytkowników w innych sesjach miały trudności z dostępem do cykli procesora. WSRM gwarantuje, że czas procesora jest rozdzielany równo pomiędzy sesje, ale angażował się dopiero wtedy, gdy jakaś sesja zaczęła się „źle zachowywać". Windows Server 2008 R2 zawiera nową funkcję o nazwie Dynamic Fair Share Scheduling (DFSS), zmieniającą sposób działania aparatu harmonogramu w jądrze systemu. Przy włączonym DFSS – czyli domyślnie – aparat harmonogramu zapewnia równe rozdzielanie czasu procesora pomiędzy sesje od samego początku. Więcej informacji na temat DFSS zawiera rozdział 3.

Wydajne wykorzystanie pamięci

Serwery RDSH rozdzielają czas procesora pomiędzy poszczególne sesje, wyrównując priorytety wszystkich procesów użytkowników i gwarantując, że żadna z sesji nie zawłaszczy całego czasu procesora tylko dlatego, że uruchomiono w niej wyjątkowo zasobożerną aplikację. Teraz przyjrzymy się, jak działa zarządzanie pamięcią, omawiając następujące zagadnienia:

- Różnice pomiędzy trybem użytkownika i trybem jądra.
- Zależności pomiędzy pamięcią fizyczną i wirtualną.
- Rola pliku wymiany w udostępnianiu dodatkowej pamięci.
- Jak menedżer pamięci optymalizuje wykorzystanie pamięci.
- Zależności pomiędzy wykorzystaniem pamięci, operacjami dyskowymi i czasem procesora.
- Jak 64-bitowa architektura wpływa na zarządzanie pamięcią wirtualną.

Istota wirtualnej przestrzeni adresowej trybu użytkownika i jądra

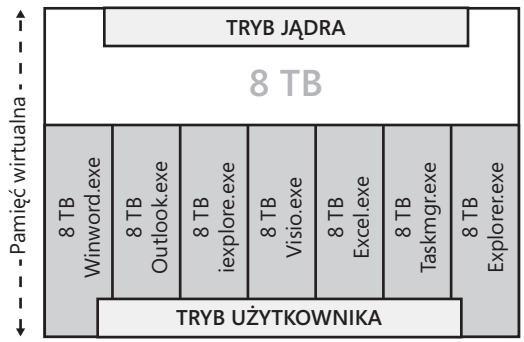
Nie moglibyśmy nic zrobić bez procesora, ale wątek uzyskujący czas procesora również nie mógłby nic zdziałać bez pamięci, w której może przechować dane. Systemy operacyjne przechowują dane, których w danym momencie potrzebują, w pamięci (dane, nad którymi aktualnie *nie* pracują, takie jak pliki, które zostały zapisane i w tym momencie nie są otwarte, są przechowywane na dyskach). Dane te mogą zawierać dane użytkownika, takie jak pliki, albo aplikacje, albo dane systemowe, takie jak wskaźniki do miejsc, w których umieszczone są właściwe dane (pamięć jest wielka – *naprawdę* wielka; nawet system operacyjny musi mieć mapę, aby się nie pogubić).

Mówiąc w uproszczeniu, pamięć komputera można rozpatrywać z dwóch punktów widzenia. Jednym jest pamięć fizyczna, czyli po prostu RAM zainstalowany w komputerze. Jeśli komputer ma 24 GB RAM, system operacyjny ma dostęp do 24 GB pamięci fizycznej (w rzeczywistości nieco mniej, gdyż część pamięci jest rezerwowana dla różnych komponentów sprzętowych). Innym podejściem jest pamięć wirtualna, limitowana przez wielkość *przestrzeni adresowej* systemu operacyjnego. W systemach 32 bitowych wielkość pamięci wirtualnej wynosiła 4 GB. Systemy 64-bitowe dysponują 16 terabajtami przestrzeni adresowej pamięci wirtualnej – 8 terabajtów dla procesów trybu użytkownika i 8 terabajtów dla trybu jądra (jeśli ktoś słyszał, że 64-bitowy system usuwa ograniczenia pamięci dla serwera terminali, ale nie był do końca pewien, co to właściwie oznacza, liczby te powinny ukazać właściwą perspektywę – terabajt to 1024 gigabajty!). Pamięć wirtualna jest obsługiwana

przez dwie fizyczne lokalizacje: pamięć fizyczną (RAM) oraz dedykowany obszar na dysku twardym, nazywany *plikiem stronicowania* (*page file*) lub *plikiem wymiany* (*swap file*). W ten sposób, nawet jeśli komputer z systemem 64-bitowym ma zainstalowane tylko 8 GB RAM, nadal dysponuje 8-terabajtowym zakresem adresów wirtualnych do bieżącego przechowywania danych.

> **Uwaga** Wykonując trochę rachunków można się przekonać, że 2 do 64 potęgi to znacznie więcej, niż 16 terabajtów – jest to 16 exabajtów. Windows (a przede wszystkim aktualnie dostępne modele procesorów) nie wspierają jednak w pełni 64-bitowego adresowania – szerokość magistrali adresowej wynosi 44 bity, co daje 2^{44}, czyli 16 terabajtów, dzielonych równo pomiędzy tryb jądra i tryb użytkownika.

Owe 16 TB przestrzeni adresowej podzielonych zostało na dwa regiony: przestrzeń jądra i przestrzeń użytkownika, zaś procesy wykorzystujące adresy w odpowiednich regionach nazywamy odpowiednio procesami trybu jądra (*kernel mode*) i trybu użytkownika (*user mode*). Przestrzeń jądra, górne 8 terabajtów, jest współdzielona przez wszystkie procesy trybu jądra. Przestrzeń użytkownika jest specyficzna dla każdego procesu trybu użytkownika. Koncepcyjnie kompozycja pamięci wygląda podobnie do rysunku 2-1. Wszystkie procesy trybu jądra *wiedzą*, że muszą dzielić wspólny obszar pamięci, ale wszystkie procesy użytkownika – nie *sesje*, ale wszystkie procesy – *sądzą*, że mają własne, osobiste 8 terabajtów pamięci trybu użytkownika. Ponieważ jednak to oznacza, że adresy pamięci wirtualnej są duplikowane pomiędzy różnymi procesami, kluczowym zadaniem menedżera pamięci jest zagwarantowanie, że poszczególne procesy trybu użytkownika nie będą wpływać na siebie nawzajem, gdy będą zapisywać dane w swoim własnym „widoku" pamięci.



Rysunek 2-1 Pamięć trybu jądra jest wspólna dla wszystkich procesów, które przechowują w niej informacje; pamięć trybu użytkownika jest specyficzna dla każdego procesu.

Zrozumienie działania trybu użytkownika i trybu jądra jest ważnym elementem na drodze do zrozumienia, jak serwer RDSH wykorzystuje pamięć.

Jak to działa

Dlaczego ważne jest, czy sterowniki działają w trybie użytkownika, czy w trybie jądra?

We wcześniejszych wersjach Windows pojawiła się zasada grupy, która wymagała od użytkowników stosowania tylko sterowników trybu jądra. Jeśli ktoś ma wątpliwości, dlaczego taka zasada może być potrzebna lub pożądana, niech czyta dalej.

Każdy komponent systemu operacyjnego Windows został zaprojektowany tak, by odwoływał się do pamięci z określonego obszaru przestrzeni adresowej, która jest podzielona na bloki. Wielkość pamięci, do której system operacyjny może mieć dostęp, zależy od schematu adresowania. Jak wspomnieliśmy, dzisiejsze 64-bitowe systemy adresują 16 terabajtów pamięci, która normalnie jest podzielona na dwie części: górne 8 TB stanowi pamięć trybu jądra, zaś dolne 8 TB to pamięć trybu użytkownika. Komponenty *trybu jądra* mają dostęp do rzeczywistych, fizycznych struktur pamięci. Komponenty *trybu użytkownika* mają dostęp tylko do mapowanego widoku tych struktur.

Struktury pamięci możemy wyobrażać sobie jako zbiór biurowych skrytek pocztowych. Komponenty trybu jądra mają dostęp do samych skrytek – fizycznych szafek zamocowanych na ścianie. Komponenty trybu użytkownika nie mają dostępu do szafek; zamiast tego mogą tylko oznaczyć porcję danych, że powinna trafić do skrytki należącej np. do Kim Abercrombie lub Michelle Pfeiffer. Komponent trybu jądra tworzy mapowanie, które wskazuje, jaka fizyczna lokalizacja jest powiązana z Kim i przekierowuje tam dane, zatem nawet jeśli szafka zostanie przeniesiona na inne piętro albo Kim dostanie nową szafkę, dane nadal trafią we właściwe miejsce. Analogicznie, jeśli komponent trybu użytkownika potrzebuje danych z jakiejś lokalizacji, nie zna on fizycznej lokalizacji tych informacji, ale odwołuje się do nich poprzez ich wirtualny adres – „Potrzebuję danych przechowywanych w szafce Kim Abercrombie". Następnie komponent trybu jądra mapuje nazwę na lokalizację skrytki i odczytuje dane. Obszar pamięci, którego dany składnik ma używać, zależy od tego, co składnik ten ma robić. Niemal wszystko, co *widzimy*, że zdarza się w komputerze, następuje w trybie użytkownika – aplikacje się otwierają, okna przesuwają, w miarę pisania pojawiają się kolejne znaki i tak dalej. Operacje przebiegające w trybie użytkownika są chronione przed sobą nawzajem, gdyż zapisują dane w wirtualnych lokalizacjach, a nie bezpośrednio w fizycznej pamięci. Komponenty trybu jądra gwarantują, że zapisy te nie będą odwoływać się do tych samych lokalizacji fizycznych. Z tego względu tryb użytkownika bywa nazywany również *trybem chronionym* (*protected mode*). Jeśli aplikacja wykonywana w trybie użytkownika ulegnie awarii, nie ma to wpływu na działanie innych aplikacji.

Komponenty trybu jądra działają nieco szybciej niż te pracujące w trybie użytkownika, gdyż nie muszą wykonywać tłumaczenia adresów wirtualnych na fizyczne, są jednak bardziej wrażliwe na błędy („nieco szybciej" w tym wypadku oznacza różnicę, której człowiek nie jest w stanie dostrzec). Odwołania trybu jądra do fizycznych struktur pamięci są wspólne dla wszystkich komponentów działających w danym

Ciąg dalszy na stronie następnej