Windows Server 2008 R2 SP1 Technical Overview

Published: October 2010

Table of Contents

Introduction to Windows Server® 2008 R2

Overview

Windows Server 2008 R2 is the latest version of the Windows Server operating system from Microsoft. Building on the features and capabilities of the Windows Server 2008 release version, Windows Server 2008 R2 allows you to create solution organizations that are easier to plan, deploy, and manage than previous versions of Windows Server.

Building upon the increased security, reliability, and performance provided by Windows Server 2008, Windows Server 2008 R2 extends connectivity and control to local and remote resources. This means your organizations can benefit from reduced costs and increased efficiencies gained through enhanced management and control over resources across the enterprise.

Using this Guide

This guide is designed to provide you with a technical overview of the new and improved features in Windows Server 2008 R2. The guide is divided into the following key technical investments that are provided in Windows Server 2008 R2:

- **Virtualization**. With its server virtualization technology, Windows Server 2008 R2 enables you to reduce costs, increase hardware utilization, optimize your infrastructure, and improve server availability.
- **Management**. Windows Server 2008 R2 reduces the amount of effort you expend managing your physical and virtual data centers by providing enhanced management consoles and automation for repetitive day-to-day administrative tasks.
- **Web**. Windows Server 2008 R2 gives you the ability to deliver rich Web-based experiences efficiently and effectively, with improved administration and diagnostics, development and application tools, and lower infrastructure costs.
- **Scalability and Reliability**. Windows Server 2008 R2 has been specifically designed to support increased workloads with less resource utilization on server computers. Windows Server 2008 R2 supports these increased workloads while enhancing reliability and security.
- **Better Together With Windows® 7**. Windows Server 2008 R2 includes technology improvements designed with Windows 7 enterprise users in mind, augmenting the network experience, security, and manageability.

As you read each section, you can identify which Windows Server 2008 R2 features and capabilities will help you create solutions for your organization. You can also see how Windows Server 2008 R2 can help you manage and protect your existing solutions.

Virtualization

Virtualization is a huge part of today's data centers. The operating efficiencies offered by virtualization allow organizations to dramatically reduce the operations effort and power consumption.

Windows Server® 2008 R2 provides the following virtualization:

- **Server and desktop virtualization provided by Hyper-V™ in Windows Server 2008 R2**. Hyper-V in Windows Server 2008 R2 is a micro-kernelized hypervisor which manages a server's system resources when hosting virtualized guests. Server virtualization allows you to provide a virtualized environment for operating systems and applications. When used alone, Hyper-V is typically used for server virtualization. When Hyper-V is used in conjunction with Virtual Desktop Infrastructure (VDI), Hyper-V is used for desktop virtualization.
- **Session virtualization**. Virtualizes a processing environment and isolates the processing from the graphics and IO, making it possible to run an application in one location but have it be controlled in another. Session virtualization may allow you to remotely access only a single application, or it may present you with a complete desktop offering multiple applications.

Note: There are other types of virtualization which are not discussed in this guide, such as application virtualization provided by Microsoft Application Virtualization version 4.5. For more information on all Microsoft virtualization products and technologies, see "Microsoft Virtualization: Home" at http://www.microsoft.com/virtualization/default.mspx.

Server and Desktop Virtualization with Hyper-V

Beginning with Windows Server 2008, server virtualization via Hyper-V technology has been an integral part of the operating system. A new version of Hyper-V, is included as a part of Windows Server 2008 R2.

Microsoft® Hyper-V in R2 supports single and multi-core x64 processors and requires 64-bit machines with AMD-V- or Intel Virtualization Technology-enabled processors. For a complete list of supported guest operating systems please see: http://support.microsoft.com/default.aspx?scid=kb;EN-US;954958.

There are two manifestations of the Hyper-V technology: Hyper-V is the hypervisor-based virtualization feature of Windows Server 2008. Microsoft Hyper-V Server is the hypervisor-based server virtualization product that allows customers to consolidate workloads onto a single physical server.

Hyper-V includes numerous improvements for creating dynamic virtual data centers, including:

- Increased availability for moving virtual machines within virtual data centers.
- Increased availability for adding and removing virtual machine storage.
- Improved management of virtual data centers.
- Simplified method for physical and virtual computer deployments by using .vhd files.

Increased Availability for Moving Virtual Machines

One of the most important aspects of any data center is providing the highest possible availability for systems and applications. Virtual data centers are no exception to the need for high availability.

Hyper-V in Windows Server 2008 R2 includes the much-anticipated Live Migration feature, which allows you to move a virtual machine between two computers running Hyper-V without any interruption of service.

Comparison of Live Migration and Quick Migration

Quick Migration is a feature found in both Windows Server 2008 Hyper-V and Windows Server 2008 R2 Hyper-V. By contrast, Live Migration is only in Windows Server 2008 R2. The primary difference between Live Migration and Quick Migration is that a Live Migration moves virtual machines without any perceived downtime or service interruption. The requirements for Live Migration and Quick Migration are very similar.

Both Live Migration and Quick Migration can be initiated by:

- The System Center Virtual Machine Manager console, if Virtual Machine Manager is managing the cluster nodes that are configured to support Live Migration or Quick Migration.

  Note: Support for Live Migration will be included in System Center Virtual Machine Manager 2008 R2.

- The Failover Cluster Management console, where an administrator can initiate a live migration.
- A Windows Management Instrumentation (WMI) script.

Integration of Live Migration and Failover Clustering

Live Migration has two core requirements: First it requires failover clustering in Windows Server 2008 R2; and second, it needs shared disk storage between cluster nodes. The shared disk storage can be provided by a vendor-based solution or by using the Cluster Shared Volumes feature in failover clustering in Windows Server 2008 R2. For more information on Cluster Shared Volumes, see "Improvements for Virtual Machine Management" in "Improved Availability for Applications and Services" later in this guide.

The following are the requirements for performing Live Migration with a failover cluster:

- Live Migration can only be performed between cluster nodes within the same failover cluster (virtual machines can only be moved between cluster nodes).
- Hyper-V must be running on the cluster nodes in the failover cluster and have access to the same shared disk storage, such as provided by Cluster Shared Volumes or vendor-based solutions.
- The .vhd files for the virtual machines to be moved by Live Migration must be stored on the same shared disk storage.

The following figure illustrates a typical Hyper-V and failover cluster configuration for supporting Live Migration.

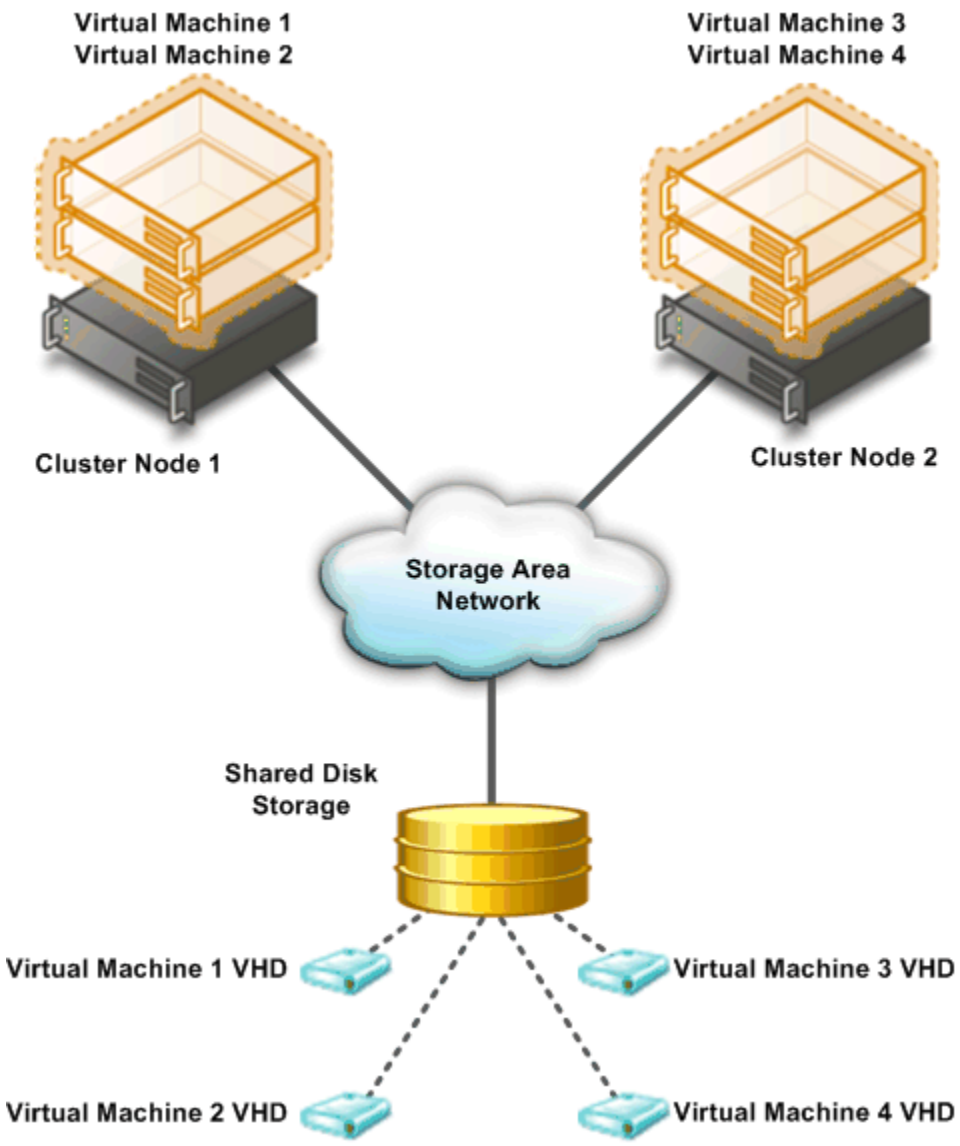

Figure 1: Typical configuration to support Live Migration

Live Migration Process

The Live Migration process is performed in the following steps:

1. A Hyper-V administrator initiates a Live Migration between the source and target cluster node.

2. A duplicate virtual machine is created on the target cluster node, as illustrated in the following figure.

   The source cluster node creates a TCP connection with the target cluster node. This connection is used to transfer the virtual machine configuration data to the target cluster node. A skeletal virtual machine VM is created on the target cluster node and memory is allocated for the destination virtual machine.

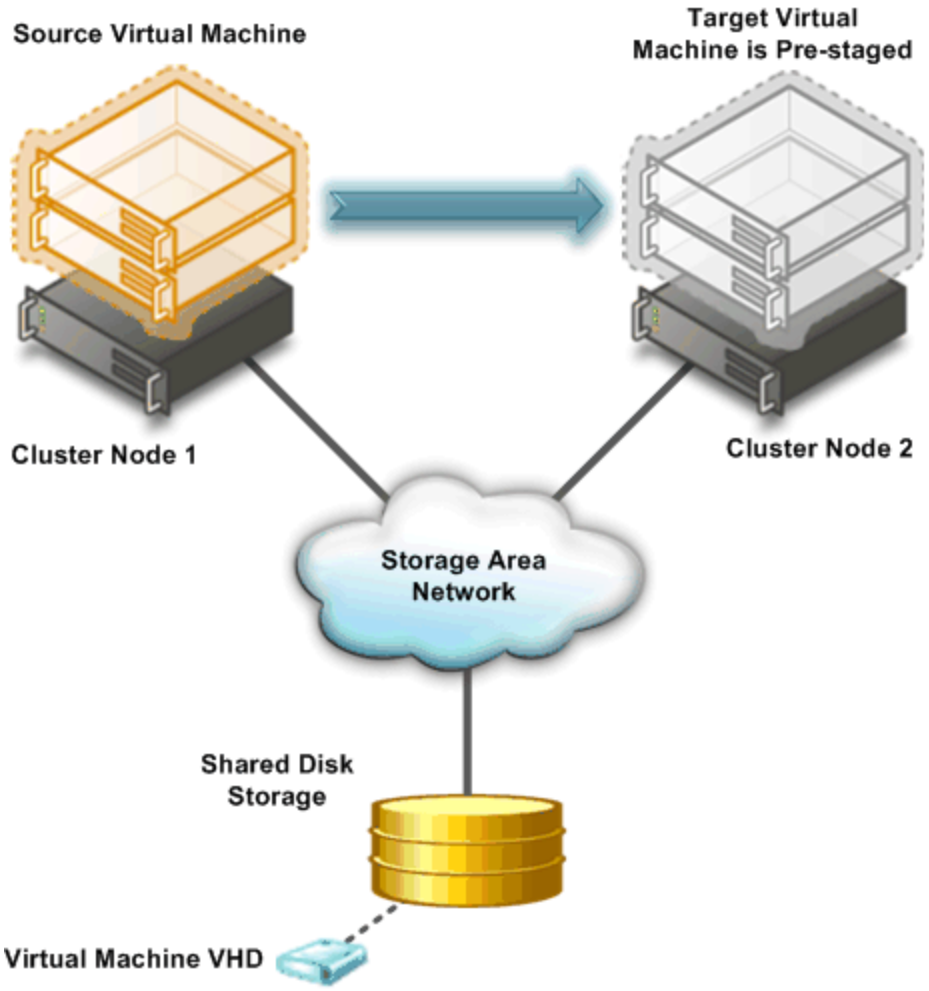

Figure 2: Creation of target virtual machine on target cluster node

3. All of the current memory in the source virtual machine is copied to the target virtual machine.

The memory assigned to the source virtual machine is copied over the network to the target virtual machine. This memory is referred to as the working set of the source virtual machine. A page of memory is 4 kilobytes in size.

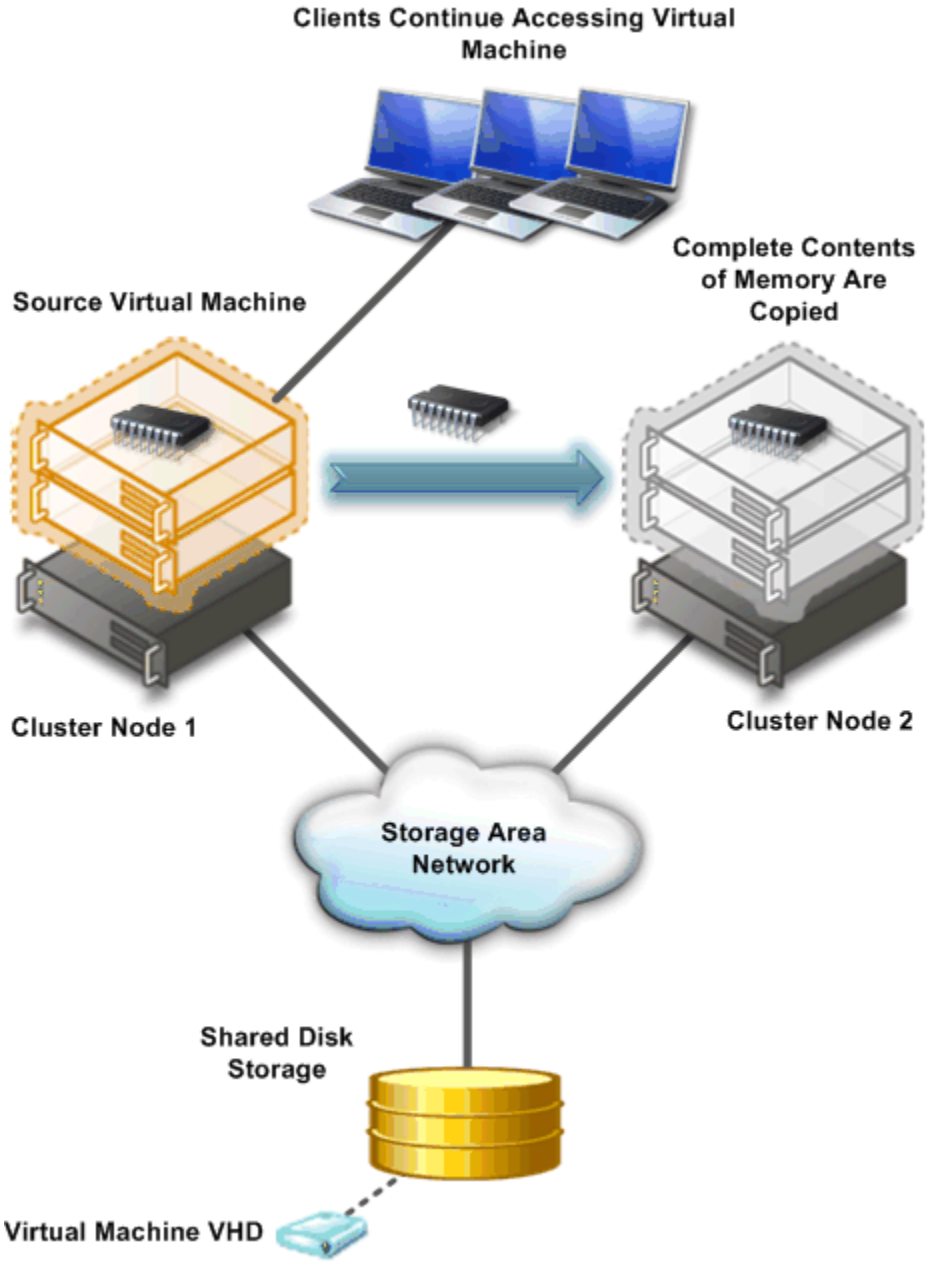

Figure 3: Initial copy of memory from source to target virtual machine

4. Clients connected to the source virtual machine continue to run on the source virtual machine and create memory pages.
5. Hyper-V tracks the memory pages and continues an iterative copy of those pages until all memory pages are copied to the target virtual machine, as illustrated in the following figure.

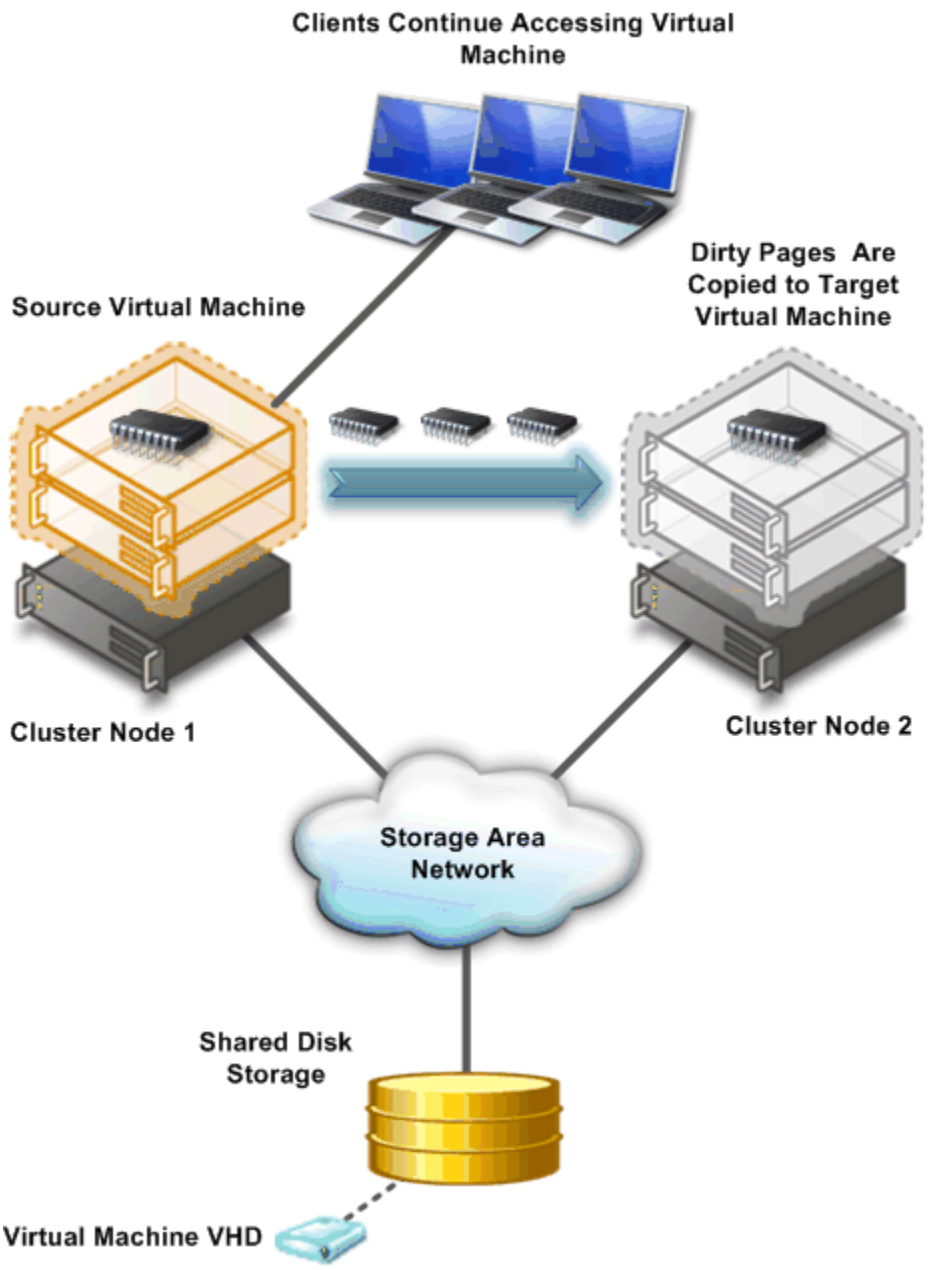

Figure 4: Iterative copy of memory from source to target virtual machine

6. When the working set of the source virtual machine is copied, the source virtual machine is paused and the remaining memory pages are copied.

Note: The live migration process may be cancelled at any point before this stage of the migration.

During this stage of the migration, the network bandwidth available between the source and target cluster nodes is critical to the speed of the migration. Live Migration requires a minimum 1 Gb/E network between cluster nodes and can take advantage of 10 Gb/E networks for even faster migrations. The faster the transmission speed between the cluster nodes, the more quickly the migration will complete.

7. The storage handles to the .vhd files or pass-through disks are transferred from the source cluster node to the target cluster node.
8. When all memory pages are copied to the target virtual machine and the storage handles are moved, the target machine is started and the clients are automatically re-directed to the target virtual machine and the source virtual machine is deleted, as illustrated in the following figure.

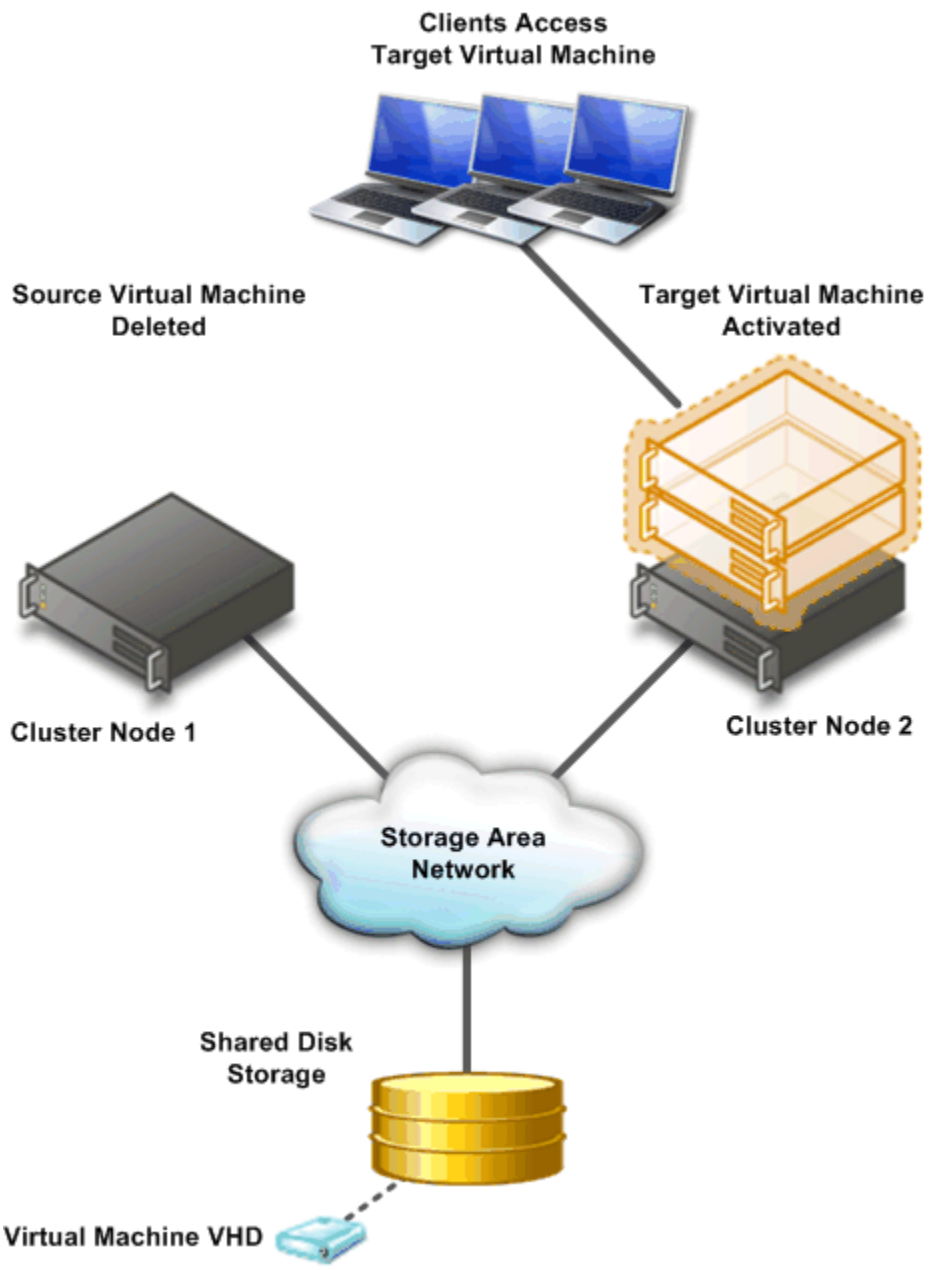

Figure 5: Final configuration after Live Migration completes

9. Force physical network switches to re-learn location of migrated virtual machine.

The Live Migration process will complete in less time than the TCP timeout interval for the virtual machine being migrated. While TCP timeout intervals vary based on network topology and other factors, most migrations will complete within a few seconds. The following variable may affect migration speed:

- Network available bandwidth between source and destination hosts
- Hardware configuration of source and destination hosts
- Load on source and destination hosts
- Network available bandwidth between Hyper-V hosts and shared storage

Increased Availability for Addition and Removal of Virtual Machine Storage

Windows Server 2008 R2 Hyper-V supports hot plug-in and hot removal of virtual machine storage. By supporting the addition or removal of Virtual Hard Drive (VHD) files and pass-through disks while a virtual machine is running, Windows Server 2008 R2 Hyper-V makes it possible to quickly reconfigure virtual machines to meet changing requirements. This feature allows the addition and removal of both VHD files and pass-through disks to existing SCSI controllers of virtual machines running the following guest operating systems:

- Windows Server 2003 x86 and x64 editions
- Windows® XP x64 edition
- Windows Server 2008 and Windows Server 2008 R2 x86 and x64 editions
- Windows Vista® x86 and x64 editions
- Windows 7® x86 and x64 editions

Note: Hot addition and removal of storage requires the guest operating system to run the Hyper-V Integration Services that is supplied with Windows Server 2008 R2.

Improved Management of Virtual Datacenters

Even with all the efficiency gains with virtualization, virtual machines still need to be managed. The number of virtual machines tends to proliferate much faster than physical computers because machines typically do not require a hardware acquisition. So, management of virtual data centers is even more imperative than ever before.

Windows Server 2008 R2 includes the following improvements that will help you manage your virtual data center:

- Reduced effort for performing day-to-day Hyper-V administrative tasks by using management consoles.
- Improved management of multiple Hyper-V servers in a virtual data center environment by using System Center Virtual Machine Manager 2008.

Reduced Administrative Effort

The Hyper-V Management console and Failover Cluster Management can be used to manage Live Migrations out of the box. But for data centers intent on leveraging the real power behind Hyper-V in R2 and Live Migration, the Microsoft System Center Virtual Machine Manager (SCVMM) adds significant value in terms of reducing overall administrative effort.

VMM can manage both Quick Migrations as well as Live Migrations and has tools that make managing disparate Hyper-V hosts easier as well. This combination gives administrators a one-stop shop when it comes to managing a dynamically changing data center. Additionally, VMM can output Windows PowerShell scripts for all console tasks, which means administrators will also be able utilize the automation advantages of PowerShell without eating a steep learning curve or being programming aficionados.

Last, SCVMM also contains an advanced reporting tool that administrators can use in dense virtualization environments to streamline decision making across the breadth of VM management, including performance, placement and purchasing.

Improved Management with System Center Virtual Machine Manager 2008 R2

Hyper-V includes the necessary management tools to manage individual server computers running Hyper-V and the virtual machines running on those computers. System Center Virtual Manager 2008 helps you manage your entire virtual data center as an administrative unit.

Some of the improved Hyper-V management features provided by System Center Virtual Machine Manager 2008 include:

- **Extended Support for Hyper-V**. System Center Virtual Machine Manager (VMM) 2008 supports all Hyper-V functionality while providing VMM-specific functions, such as the Intelligent Placement, the Self-Service Portal, and the Integrated Library.
- **Automated responses to virtual machine performance problems and failures**. The Performance and Resource Optimization (PRO) feature in VMM 2008 can dynamically respond to failure scenarios or poorly configured components that are identified in hardware, operating systems, or applications. When combined with PRO-enabled

Management Packs and System Center Operations Manager 2007, you can receive automatic notifications if a virtual machine, operating system, or application is unhealthy.

- **Improved availability for virtual machines**. VMM 2008 includes expanded support for failover clusters that improves the high-availability capabilities for managing mission-critical virtual machines. VMM 2008 is now fully cluster-aware, meaning it can detect and manage Hyper-V host clusters as a single unit. New user-friendly features, such as automatic detection of added or removed virtual hosts and designating high-availability virtual machine with one click, which helps reduce your administrative effort.
- **Quick Storage Migration**. Quick Storage Migration enables migration of a VM's storage both within the same host and across hosts while the VM is running with a minimum of downtime,

Simplified Method for Physical and Virtual Computer Deployments

Historically, deploying operating systems and applications to physical and virtual computers has used different methods. For virtual computers, the .vhd file format has become a *de facto* standard for deploying and interchanging pre-configured operating systems and applications.

Windows Server 2008 R2 also supports the ability to boot a computer from a .vhd file stored on a local hard disk. This allows you to use pre-configured .vhd files for deploying virtual and physical computers. This helps reduce the number of images that you need to manage and provides an easier method for your testing deployment prior to deployment in your production environment.

Hyper-V Processor Compatibility Mode for Live Migration

As the scope of virtualization increases rapidly in today's enterprise, customers have been chafing against hardware restrictions when performing VM migrations across physical hosts. With previous versions of Hyper-V, such migrations could essentially be performed only across hosts with an identical CPU architecture. Windows Server 2008 R2 Hyper-V, however, introduces a new capability, dubbed processor compatibility mode for live migration.

Processor compatibility mode enables IT administrators to freely migrate VMs across physical hosts with differing CPU architectures as long as those architectures are support hardware assisted virtualization and within the same CPU product family, meaning Intel-to-Intel or AMD-to-AMD, but not Intel-to-AMD or vice versa. Processor compatibility mode was developed to address three basic customer scenarios:

1. A virtual machine running on Host A must be moved to Host B for effective load balancing across the physical hosts.
2. In a host cluster of identical processors, one has a hardware failure. The systems administrator purchases another server and adds it to the cluster; however the new server is using newer CPU technology than the original cluster members, yet must still support VM migrations.
3. A virtual machine running on Host A is saved. Later, the systems administrator needs to restore that VM to active memory on another Hyper-V host, which may not have the identical CPU configuration as the original host.

How Processor compatibility mode works

When a Virtual Machine (VM) is started on a host, the Hypervisor exposes the set of supported processor features available on the underlying hardware of that host to the VM. These sets of processor features are called the guest visible processor features. This set of processor features is available to the VM until the VM is restarted. When a running VM is migrated to another host, Hyper-V first compares verifies processor features currently available to the VM are also available on the destination host. If the destination processor does support all of the features available to the VM, the migration will fail.

With processor compatibility mode enabled, Hyper-V only exposes the guest VM to processor features that are available across all processors of the same processor architecture, i.e. AMD-to-AMD or Intel-to-Intel. This allows the VM to be migrated to any hardware platform of the same processor architecture. Processor features are "hidden" by the Hypervisor by intercepting a VM's CPUID instruction and clearing the returned bits corresponding to the hidden features.

When a VM in a processor compatibility mode is started, the following processor features are hidden from the VM:

Host running AMD based processor	Host running Intel based processor
SSSE3, SSE4.1, SSE4.A, SSE5, POPCNT, LZCNT, Misaligned SSE, AMD 3DNow!, Extended AMD 3DNow!	SSSE3, SSE4.1, SSE4.2, POPCNT, Misaligned SSE, XSAVE, AVX

Improved Virtual Networking Performance

The new Hyper-V leverages several new networking technologies contained in Windows Server 2008 R2 to improve overall VM networking performance. Two key examples are support for Jumbo Frames and new support for the Virtual Machine Queue (VMQ).

Support for Jumbo Frames was also introduced with Windows Server 2008. Hyper-V in Windows Server 2008 R2 simply extends this capability to VMs. So just like in physical network scenarios, Jumbo Frames add the same basic performance enhancements to virtual networking. That includes up to 6 times larger payloads per packet, which improves not only overall throughput but also reduces CPU utilization for large file transfers.

VMQ allows the host's network interface card (NIC) to DMA packets directly into individual VM memory stacks. Each VM device buffer is assigned a VMQ, which avoids needless packet copies and route lookups in the virtual switch. Essentially, VMQ allows the host's single NIC card to appear as multiple NICs to the VMs, allowing each VM its own dedicated NIC. The result is less data in the host's buffers and an overall performance improvement to I/O operations.

Improved Virtual Machine Memory Management

Windows Server 2008 R2 SP1 introduces Hyper-V Dynamic Memory. Dynamic memory is a memory management enhancement for Hyper-V that enables customers to increase the efficiency of memory usage. By dynamically and securely adjusting the distribution of memory among virtual machines, Dynamic Memory helps enable the potential for higher consolidation ratios per physical host server.

Dynamic memory dynamically increases and decreases the memory allocated to VMs based on usage. This results in more efficient utilization of memory and facilitates greater consolidation ratios of virtual machines. Dynamic memory is designed for production use and enables customers to obtain benefits on their servers with predictable performance and consistent scalability for their production deployment environments.

Dynamic Memory has requirements on both the host side and the guest operating system side. The following sections summarize these requirements for the beta release of Service Pack 1.

Host Requirements for Dynamic Memory

In order to be able to use the Dynamic Memory feature on a Hyper-V host, Service Pack 1 must be applied to one of the following virtualization platforms:

- Windows Server 2008 R2 with the Hyper-V server role installed

- Microsoft Hyper-V Server 2008 R2

Guest Requirements for Dynamic Memory

The following Windows server operating systems support Dynamic Memory when installed as the guest operating system on a virtual machine:

- Windows Server 2008 R2 Standard Edition SP1*
- Windows Server 2008 R2 Enterprise Edition SP1
- Windows Server 2008 R2 Datacenter Edition SP1
- Windows Server 2008 R2 Web Edition SP1*
- Windows Server 2008 Standard Edition SP2*
- Windows Server 2008 Enterprise Edition SP2
- Windows Server 2008 Datacenter Edition SP2
- Windows Server 2008 Web Edition SP2*
- Windows Server 2003 R2 Standard Edition SP2 or higher*
- Windows Server 2003 R2 Enterprise Edition SP2 or higher
- Windows Server 2003 R2 Datacenter Edition SP2 or higher
- Windows Server 2003 R2 Web Edition SP2 or higher*
- Windows Server 2003 Standard Edition SP2 or higher*
- Windows Server 2003 Enterprise Edition SP2 or higher
- Windows Server 2003 Datacenter Edition SP2 or higher
- Windows Server 2003 Web Edition SP2 or higher*

Note: The Beta release of Service Pack 1 does not support Dynamic Memory for the operating systems marked with an asterisk (*) above. However, support for Dynamic Memory for these operating systems will be added in a future release of SP1.

Note: Dynamic Memory is supported for both the x86 and x64 architectures of Windows Server 2003, Windows Server 2003 R2 and Windows Server 2008.

The following **Windows client operating systems** for both x86 and x64 architecture also support Dynamic Memory when installed as the guest operating system on a virtual machine:

- Windows® 7 Enterprise Edition
- Windows 7 Ultimate Edition
- Windows Vista® Enterprise Edition SP2
- Windows Vista Ultimate Edition SP2

Terminal Services Becomes Remote Desktop Services Session Virtualization

Terminal Services is one of the most widely used features in previous versions of Windows Server. Terminal Services makes it possible to remotely run an application or an entire desktop in one location but have it be controlled and managed in another. Microsoft has evolved this concept considerably in Windows Server 2008 R2, so we've decided to rename Terminal Services to Remote Desktop Services (RDS) to better reflect these exciting new features and capabilities. The goal of RDS is to provide both users and administrators with both the features and the flexibility necessary to build the most robust access experience in any deployment scenario.

In addition to enabling a virtual desktop infrastructure (VDI), Remote Desktop Services in Windows Server 2008 R2 covers the same basic technology features as did Terminal Services, which is now referred to as session virtualization. The table below summarizes the new names for TS-to-RDS technologies in R2.

Table 1: New Remote Desktop Services Names for Corresponding Terminal Services Names

Terminal Services name	Remote Desktop Services name
Terminal Services	RDS Session Virtualization
Terminal Services RemoteApp	RemoteApp
Terminal Services Gateway	Remote Desktop Gateway
Terminal Services Session Broker	Remote Desktop Connection Broker
Terminal Services Web Access	Remote Desktop Web Access
Terminal Services CAL	Remote Desktop Services CAL
Terminal Services Easy Print	Remote Desktop Easy Print

Remote Desktop Services and Virtual Desktop Infrastructure

To expand the Remote Desktop Services feature set, Microsoft has been investing in the Virtual Desktop Infrastructure, also known as VDI, in collaboration with our software and hardware partners. VDI is a centralized desktop delivery architecture, which allows customers to centralize the storage, execution and management of a Windows desktop in the data center. It enables Windows 7 Enterprise and other desktop environments to run and be managed in virtual machines on a centralized server.

Increasingly businesses aim to enable their employees and contractors to work from home or from an offshore, outsourced facility. These new work environments provide better flexibility, cost control and lower environmental footprint but increase demand for security and compliance so that precious Corporate data is not at risk.

To answer these challenges, Microsoft has updated the Terminal Services Connection Broker, now called Remote Desktop Connection Broker. The new Remote Desktop Connection Broker extends the Session Broker capabilities already found in Windows Server 2008, and creates a unified admin experience for traditional session-based remote desktops and new virtual machine-based remote desktops.

The two key deployment scenarios supported by the Remote Desktop Connection Broker are persistent (permanent) VMs and pooled VMs. In the case of a persistent VM, there is a one-to-one mapping of VMs to users; each user is assigned a dedicated VM which can be personalized and customized, and which preserves any changes made by the user. Today, most early adopters of VDI deploy persistent VMs as they provide the greatest flexibility to the end user. In the case of a pooled VM, a single image is replicated as needed for users;

user state can be stored via profiles and folder redirection, but will not persist on the VM once the user logs off. In either case, the in-box solution supports storage of the image(s) on the Hyper-V host.

The Remote Desktop Connection Broker has been designed as an extensible platform for partners; it includes extensive APIs for partner value-add around manageability and scalability of the brokering solution. Specifically, extensibility points include the ability for partners to create policy plug-ins (e.g. for determining the appropriate VM or VM pool), filter plug-ins (e.g. for preparing a VM to accept RDP connections) and resource plug-ins (e.g. for placing a VM on the proper host based on the host's load). RDS addresses all these challenges by incorporating the following features:

Improved User Experience

For both VDI and traditional session virtualization (formerly know as Terminal Services) the quality of user experience is more important than ever before. Windows Server 2008 R2 greatly improves the end user experience for VDI and session virtualization through new Remote Desktop Protocol capabilities. New capabilities enabled with Windows Server 2008 R2 SP1 and Microsoft RemoteFX help create a local-like user experience for remote users from any client device, rich or thin.

Improved RemoteApp and Desktop Connections

New RemoteApp & Desktop Connection (RAD) feeds provide a set of resources, such as RemoteApp programs and Remote Desktops. These feeds are presented to Windows 7 users via the new RemoteApp & Desktop Connection control panel, and resources are tightly integrated into both the Start menu and the system tray.

The improved RemoteApp and Desktop Connections features in Windows Server 2008 R2 and Windows 7 provide the following improvements:

- **Extends Remote Desktop Services to enable a virtual desktop infrastructure (VDI).** The in-box Remote Desktop Services capability is targeted at low-complexity deployments and as a platform for partner solutions, which can extend scalability and manageability to address the needs of more demanding enterprise deployments. The scope of the VDI architecture can include the following technologies and licenses to provide a comprehensive solution:
  - Hyper-V
  - Live Migration
  - System Center Virtual Machine Manager
  - Microsoft Application Virtualization in Microsoft Desktop Optimization Pack (MDOP).

- Microsoft RemoteFX
- Windows Virtual Desktop Access (VDA) licensing

- **Provides simplified publishing of, and access to, remote desktops and applications.** The feeds described above provide access in Windows 7, but using the new RemoteApp & Desktop Web Access, users will also be able connect to these resources from Windows Vista and Windows XP using a web page.
- **Improved integration with Windows 7 user interface**. Once accessed, RAD-delivered programs and desktops show up in the Start Menu of Windows 7 with the same look and feel of locally installed applications. A new System Tray icon shows connectivity status to all the remote desktop and RemoteApp connections to which the user is currently subscribed. The experience is designed so that many users won't be able to tell the difference between a local and remote application.

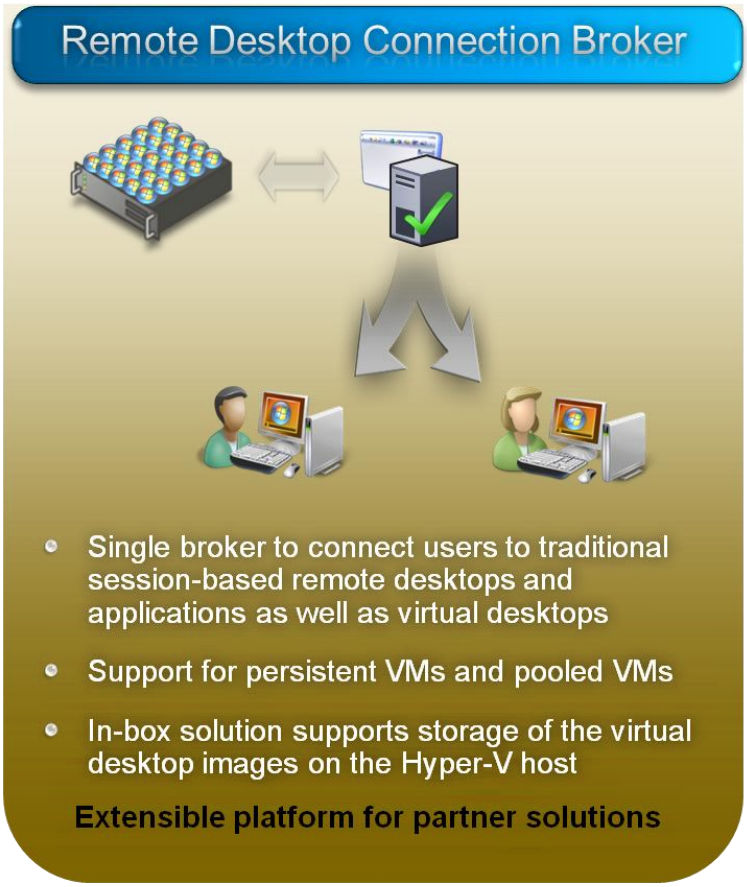

Figure 6: Updates to the Remote Desktop Services Connection Broker

Improved User Experience Through New Remote Desktop Protocol Capabilities

These new capabilities, enabled with Windows Server 2008 R2 in combination with Windows 7, improve significantly the experience of remote users, making it more similar to the experience enjoyed by users accessing local computing resources. These improvements include:

- **Multimedia Redirection**: Provides high-quality multimedia by redirecting multimedia files and streams so that audio and video content is sent in its original format from the server to the client and rendered using the client's local media playback capabilities.
- **True multiple monitor support**: Enables support for up to 10 monitors in almost any size, resolution or layout with RemoteApp and remote desktops; applications will behave just like they do when running locally in multi-monitor configurations.
- **Audio Input & Recording**: VDI supports any microphone connected to a user's local machine, enables audio recording support for RemoteApp and Remote Desktop.
- **Aero® Glass support**: VDI provides users with the ability to use the AeroGlass UI for client desktops; ensuring that remote desktop sessions look and feel like local desktop sessions.
- **Enhanced bitmap acceleration**: 3D and other rich media applications such as Flash or Silverlight™ will render on the server and will be remoted using bitmaps.
- **Improved audio/video synchronization**: RDP improvements in Windows Server 2008 R2 are designed to provide closer synchronization of audio and video in most scenarios.
- **Language Bar Redirection**: Users can easily and seamlessly control the language setting (e.g. right to left) for RemoteApp programs using the local language bar.
- **Task Scheduler:** This adds the ability in Task Scheduler to ensure that scheduled applications never appear to users connecting with RemoteApp. This reduces user confusion.
- **NEW in Windows Server 2008 R2 Service Pack 1: Microsoft RemoteFX** (see page 28)

While RAD improves the end-user experience, RAD also reduces the desktop and application management effort by providing a dedicated management interface that lets IT managers assign remote resources to users quickly and dynamically. Windows Server 2008 R2 includes the following RAD management capabilities to help reduce administrative effort:

- **RemoteApp & Desktop Connections control panel applet.** Users can easily connect to RemoteApp programs and Remote Desktops using the RemoteApp & Desktop Connections control panel applet in Windows 7.
- **Single administrative infrastructure.** Both RemoteApp & Desktop connections and RemoteApp and Desktop Web Access are managed from a single management console. This ensures that connections can still be used from Windows XP and Vista by using a Web page.
- **Designed for computers that are domain members and standalone computers:** The RemoteApp & Desktop feature is easy to configure and use for computers that are members of Active Directory domains and for standalone computers**.**
- **Always up to date.** Once a workspace is configured, that workspace keeps itself up to date until it is removed from the user's desktop. When an admin adds an application or update it automatically appears on users' Start menu and via that user's Web Access page.
- **Single sign-on experience within a workspace.** Ensures that only a single logon is required to access all applications and resources with a RAD connection.
- **RemoteApp & Desktop Web Access.** This capability provides full integration with RemoteApp & Desktop Connections to ensure a consistent list of applications is available to the user at all times, no matter the desktop OS used. The default web page provides a fresh and inviting look and feel and includes a new Web-based login with integrated single sign-on.

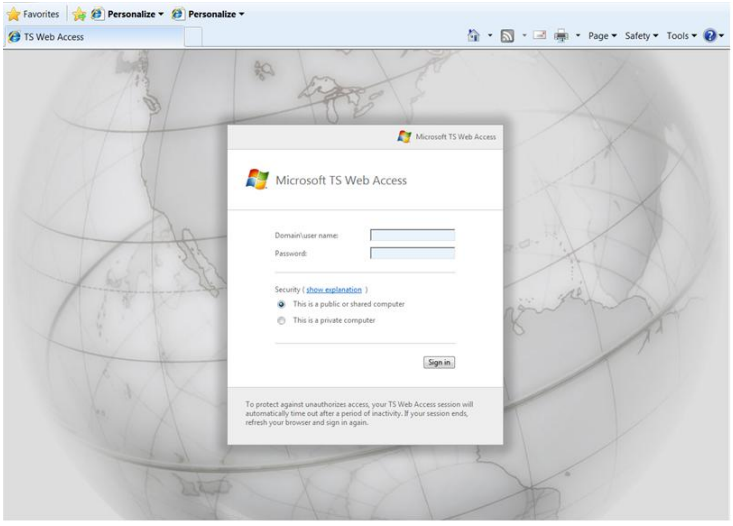

Figure 7: Remote Desktop Services Web Access expands RDS features cross-OS

Administrators faced with larger RAD deployment scenarios will also find additional management features in Windows Server 2008 R2's Remote Desktop Services aimed at improving the management experience for all existing scenarios previously addressed by Terminal Services as well as the exciting new scenarios available via RAD. These improved management features include:

- **Windows PowerShell Provider.** Easily manage multiple servers and repetitive tasks - almost all Remote Desktop Services administrative tasks can now be scripted; view and edit configuration settings for the Remote Desktop Gateway, Remote Desktop Server and more.
- **Profile Improvements.** The user profile cache quota removes the need to delete profiles at logoff, speeding up user logon. Group policy caching can now be performed across an RDS farm to speed up group policy processing during logon
- **Microsoft Installer (MSI) compatibility.** Microsoft has fixed multiple MSI-related issues with Windows Server 2008's Terminal Services to ensure that MSI install packages can be installed normally and that per-user install settings are correctly propagated. The updates also remove the need to put the server in 'install mode', meaning users no longer need to be logged off during RAD management operations.
- **Remote Desktop Gateway.** RDG securely provides access to RAD resources from the Internet without the need for opening additional ports or the use of a VPN. RDG provides this by tunneling RDP over HTTPS and incorporating several new security features:
    - **Silent Session Re-authentication.** The Gateway administrator can now configure the RDG to run periodic user authentication and authorization on all live connections. This ensures that any changes to user profiles are enforced. For users whose profiles haven't changed, the experience is seamless.
    - **Secure device redirection.** The Gateway administrator can be assured that device redirection settings are always enforced even from unmanaged clients like kiosks.
    - **Pluggable Authentication.** For corporations that have specific need to implement their own authentication and authorization technologies, these customers now have the flexibility to plug-in their preferred authentication/authorization mechanisms.
    - **Idle & session timeout.** Administrators now have the flexibility of disconnecting idle sessions or limiting how long users can be connected.
    - **Consent Signing.** If your business demands that remote users adhere to legal terms & conditions before accessing corporate resources, the consent signing feature helps you do just that.

- **Administrative messaging.** The Gateway also provides the flexibility to provide broadcast messages to users before launching any administration activities such as maintenance or upgrades.

Partners and Independent Software Vendors (ISVs) also get tools with the new service to more easily enable third-party software manufacturers to build RAD-optimized products. These tools include:

- **RemoteApp & Desktop Web Access Customization.** It is now possible to easily extend the look and feel of web access by both customers and partners using support for cascading style sheets. Developers can also create custom Web sites that consume the RAD connection XML feed and transform these with XSLT.
- **RemoteApp & Desktop Connection.** Though RAD connections are currently only used for Remote Desktop Services, it is possible to extend both the server-side infrastructure and Windows 7 client shell to add support for any type of application or service – even ones that don't use RDP or remoting protocols. This provides a single UI and point of discoverability for any service.
- **Session broker extensibility.** The session broker offers broad extensibility to enable customers and ISVs to take advantage of the built-in RDP redirection features while providing significant additional unique value through the various types of plug-ins; for example:
  - Policy (*policy plug-in*), which determines the proper farm or VM for a connection,
  - Load Balancing (*filter plug-in*), which chooses the proper endpoint based on load, and
  - Orchestration (*filter plug-in*), which prepares a VM to accept RDP connections.

Improved User Experience When Accessing Media Rich Content and hardware-accelerated graphics applications

Trends in current IT environments include faster network speeds, massively parallel processors, and an increasing diversity of client devices. The user experience for today's user includes increased richness in graphics, including 3D user interfaces, video, animations, and other rich media content. Also, hardware acceleration for these user experiences, especially of 3D business applications such as Office 2010 or Bing3D maps, is becoming common place.

Microsoft RemoteFX is a feature in Windows Server 2008 R2 SP1 Remote Desktop Services that enables connected users to access media-rich virtual and session-based desktops over the network from a broad range of client devices. RemoteFX helps the user experience for

remote session in Remote Desktop Services more closely mirror the user experience on a local computer running Windows.

RemoteFX delivers value in the following areas:

3D Graphical support for VDI (RDVH) solutions using Virtual GPU. The enhanced features in RemoteFX allow remote users to have access to all the user experience features in all Windows operating systems, especially Windows 7. This includes the 3D aspects of Aero Glass and other DirectX/Direct3D applications.

The following figure illustrates the user experience in Remote Desktop Services in Windows Server 2008 R2 SP1 for a Windows 7 guest operating system in VDI. Remote users are able to use all the graphical features that Windows 7 provides.

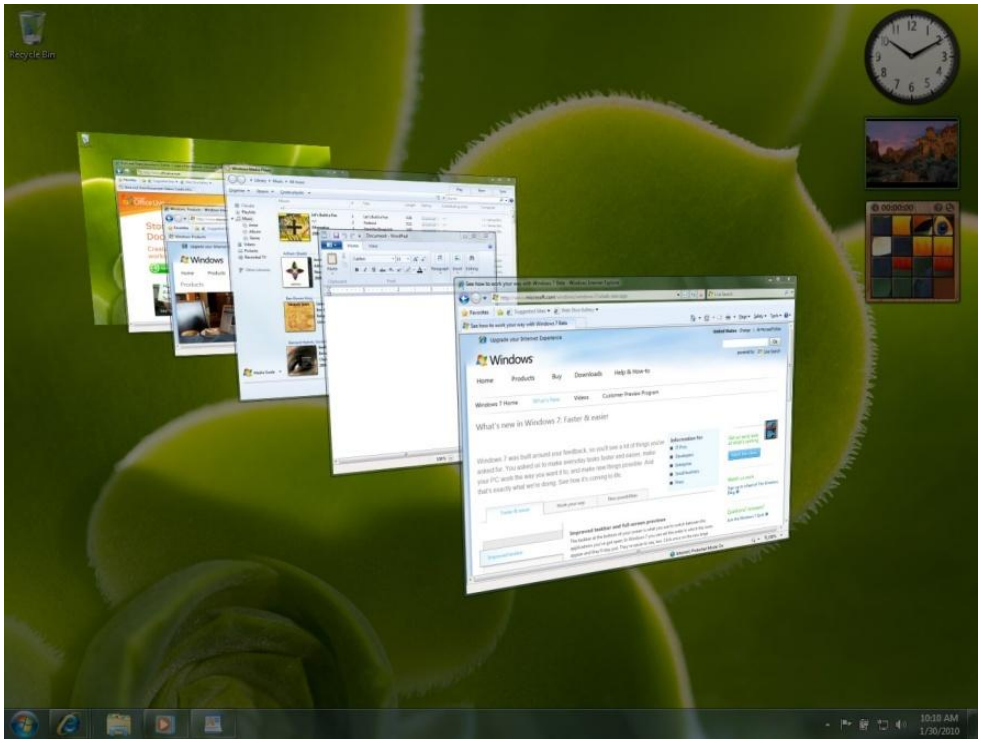

Figure 8: User experience in Windows 7 VDI with Windows Server 2008 R2 SP1

The server running Windows Server 2008 R2 SP1 renders the graphics content locally using its graphic processing unit (GPU) for the Windows 7 Enterprise or Ultimate VDI instances and then sends the rendered bitmap content to the client. Ultra-thin clients or

even LCD panels can be used to display RemoteFX-based content because the client is only displaying the content and not performing the rendering itself.

- **Improved efficiency over RDP for demanding remote workloads**. The server-side encode of the graphical content can be performed more efficiently by the RemoteFX codec within RDP and handled in three ways:
  - **Software-based encode codec (Both RDSH and RDVH)**. The processors in the server encodes the graphics by running a software-implementation of the RemoteFX codec. This method is the most demanding on the server processor resources.
  - **Graphics processor-based encode codec (RDVH only)**. The graphics processor on a graphics adapter in the server encodes the RemoteFX codec. This method reduces the demands on the server processor resources, but increases the demands on the graphics processor. This can only be done in a VDI (RDVH) environment, not RDSH.
  - **RemoteFX ASIC-based encode codec (Both RDSH and RDVH)**.. A RemoteFX Application-Specific Integrated Circuit (ASIC) is a hardware implementation of the RemoteFX codec. This method is the least demanding on the server processor resources and the graphic processor resources. This will enable a similar benefit to the server that TCP offload provides today for TCP/IP networking.
- **Improved support for a broader range of devices**. Because of the reduced hardware requirements at the endpoint, RemoteFX provides support for a broader range of devices, including Windows-based computers, traditional thin clients, ultra-light thin clients, mobile devices, and dedicated access devices (such as an LCD display).
  - **Software-based decode codec**. Like the server protocol encode, RemoteFX also provides a decode codec. This will result in an updated MSTSC client and available on all versions of Windows 7 as RDP 7.1
  - **RemoteFX ASIC-based decode codec**. A RemoteFX Application-Specific Integrated Circuit (ASIC) is a hardware implementation of the RemoteFX decode codec. This method is also useful when wanting to create ultra-light solid state thin clients or specialized RemoteFX-enabled devices
- **Generic USB Redirection for VDI (RDVH only).** RemoteFX enables generic redirection of nearly any USB device in a Windows 7 Enterprise or Ultimate VDI session which can enable support for multifunction printers and other mainstream USB devices.

RemoteFX can provide enhanced features for VDI solutions and for session virtualization. In VDI (RDVH) solutions, RemoteFX provides an improved user experience for users running

Windows 7 and applications in virtualized environments on Hyper-V. In remote session (RDSH) solutions, RemoteFX provides an improved user experience for remote desktop sessions.

Note: Session Virtualization with RemoteFX supports all content types except for 3D content.

Management

The ongoing management of servers in the data center is one of most time consuming task facing IT professionals today. Today's combination of virtual and physical management needs can make this an even more daunting task without proper planning and tools, because management strategies must support the management of both physical and virtual environments. Additionally, these management strategies must address and track power consumption and green IT policies.

Because of these customer challenges, a key design goal for Windows Server® 2008 R2 is to reduce the day-to-day management chores of Windows Server 2008 R2 as well as to ease the administrative effort for common day-to-day operational tasks. A final but critical design component was that administrative tasks should be doable either on the server locally or remotely.

Thus, the overall management improvements in Windows Server 2008 R2 include the following:

- Improved data center power consumption management
- Improved remote administration
- Reduced administrative effort for administrative tasks performed interactively
- Enhanced command-line and automated management by using Windows PowerShell™ version 2.0
- Improved identity management provided by Active Directory® Domain Services (AD DS) and Active Directory Federated Services
- Improved compliance with established standards and best practices

Improved Data Center Power Consumption Management

With the proliferation of physical computers in data centers, power consumption is of paramount importance. In addition to the cost-saving associated with reducing power consumption, many data centers are constrained by the number of computers they can support in their data center by the actual power available to the data center. Therefore reducing your power consumption also allows you to support more physical computers while using the same amount of power, or less power, than before.

Window Server 2008 R2 includes the following improvements for reducing power consumption:

- Reduced power usage of individual servers
    - A new PPM engine
    - Storage power management
    - Additional incremental power saving features
- The ability to measure, manage, and budget power usage across the system

Microsoft has also added an additional, optional qualifier to the Designated for Windows Server 2008 R2 qualification logo to indicate enhanced power management support. Through use of the qualifier, OEMs can alert customers to servers that work in collaboration with Windows Server 2008 R2 power capabilities to provide optimal power efficiency.

Improve the Power Efficiency of Individual Servers

Windows Server 2008 R2 helps improve the power efficiency of individual servers through a variety of incremental improvements. To quantify the power savings, Microsoft measured power consumption of Windows Server 2003 and Windows Server 2008 R2 using a representative online transaction processing (OLTP) workload. Throughput was gradually throttled up across the utilization range of the systems, from idle up to 100 percent utilization.

Measuring power usage only when hardware is fully utilized does not reflect real-world usage; average utilization for many servers is 5 to 15 percent. Figure 15 shows the results, which demonstrate that the many servers that operate in a range of utilization levels will benefit from improved power efficiency of Windows Server 2008 R2.

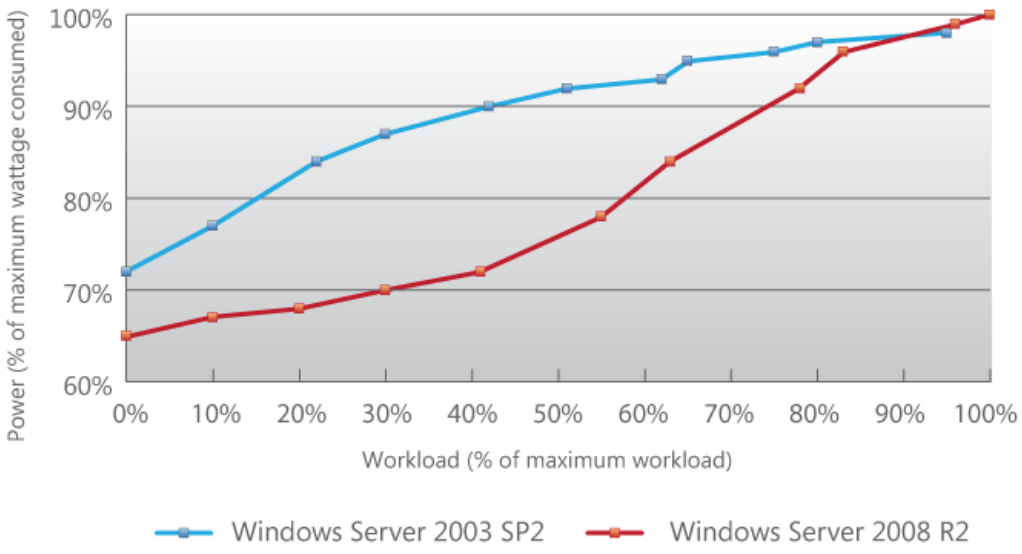

Figure 9: Power savings with Windows Server 2008 R2

Processor Power Management

The PPM engine in Windows Server 2008 R2 has been re-written and improved. It now provides the ability to fine-tune the processor's speed and power consumption to match current demands. New parameters for PPM—which are configurable by administrators—further improve power efficiency.

Core parking is a feature that enables Windows Server 2008 R2 to reduce multi-core processor power consumption by consolidating processing onto fewer processor cores and suspending the inactive cores. The workloads of every logical core in a server are tracked relative to all the others. The workloads of cores that are not being fully utilized can be suspended, and their workloads are then shifted to alternate cores. Keeping the unutilized cores in an idle state reduces the system power consumption. When additional processing power is required, the system activates the idle processor cores to handle the increased processing requirements.

Storage Power Management

Another strategy for reducing power used by individual servers is to centralize their storage by using a Storage Area Network (SAN), which has a higher storage-capacity-to-power-consumption ratio than a typical server. A SAN also makes more efficient use of the available disk space, because any server can have access to the available storage on the SAN.

Windows Server 2008 R2 greatly improves access to storage on SANs, and also adds the following enhancements:

- **ATA Slumber feature**—This feature is integrated with the power management framework to use the new power states (partial and active).
- **Optimized link power management for SATA disks**—This feature helps reduce power usage for managing the communication bus link between the hard disk and the chipset.
- **Asynchronous notification of media change for optical devices**—Windows Server 2008 R2 provides asynchronous notification of drive media changes. This means that commands are not repeatedly being sent to check for media changes; less communication with the drive means less power is drawn.
- **Support for "remove on delete"**—Windows Server 2008 R2 includes support for storage devices that work with solid state drives that can power down unused RAM when a file system deletes files, thus saving power.

Windows Server 2008 R2 also supports the ability to boot from a SAN, which eliminates the need for local hard disks (local storage) in the individual server computers and decreases power consumption as a result (see the following figure).

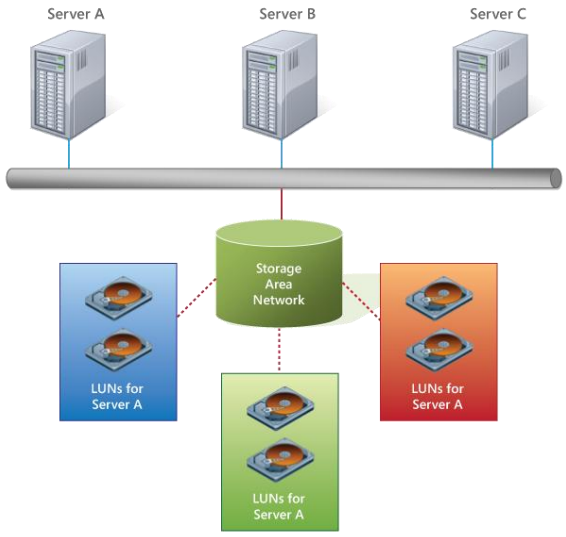

Figure 10: Each server without local storage, and each consuming less power

Additional Power Saving Features

Windows Server 2008 R2 introduces Intelligent Timer Tick Distribution (or Tick Skipping). This feature extends processor idle or deep C-states (processor sleep states within the ACPI specification, with C3 set as the deepest-sleep state and C0 as the operating state) by not activating the CPU unnecessarily, thus saving power. One processor handles the periodic system timer tick; other processors are signaled only as necessary. (Non-timer interrupts, however, will still activate sleeping processors.)

The amount of background work that is performed by the operating system has also been reduced in Windows Server 2008 R2. This also allows processors to better utilize the deep C-states, in which the processor consumes very little energy but requires time to return to an operational state.

Most of these technologies can also be leveraged in virtualization scenarios, letting you maximize the power efficiency of your virtualized environments as well as your physical systems.

Measure and Manage Power Usage Across the Organization

Windows Server 2008 R2 also helps provide businesses with the capability to better measure and manage power consumption, both locally and remotely across the enterprise. In

conjunction with server OEMs, Microsoft is pursuing an ACPI standards-based approach to the features that provide these capabilities.

Remote Manageability of Power Policy

Key in Windows Server 2008 R2 is the greatly enhanced ability to measure, manage, and budget energy usage for individual servers and across the entire server environment.

For centralized power policy management, there are new features in Group Policy for Windows Server 2008 R2, including an improved user interface, additional policy settings, and Windows PowerShell™ cmdlets for Group Policy, which provide the ability to manage Group Policy from the Windows PowerShell command line and to run Windows PowerShell scripts during logon and startup.

Windows Server 2008 R2 supports the configuration of power policy, both locally and remotely, through Windows Management Instrumentation (WMI), providing a powerful and convenient way to capture and report information about power consumption, and in turn making power consumption data an actionable metric.

WMI, the infrastructure for management data and operations on Windows-based operating systems, exposes the data that is gathered to users, scripts, or management tools in a manner that is compliant with the Distributed Management Task Force (DMTF) management profiles, ensuring interoperability across the entire IT environment.

Windows Server 2008 R2 provides a new power namespace, root\cimv2\power, which enables code and scripts to query power data on compliant systems. This is useful for IT administrators who use WMI queries in scripts to monitor and administer their infrastructure.

IT workers responsible for power management can control power policies and receive power condition events, providing them with the data they need to make informed and timely power management decisions.

Power metering and budgeting in Windows Server 2008 R2 require no additional drivers or hardware changes, only hardware platform support.

In-Band Power Metering and Budgeting

The new power features introduce new opportunities for managing power consumption. An administrator can use the performance monitor on a server to view the moment-by-moment power consumption, or, in a more likely scenario, the IT administrator can write a script or use Microsoft® System Center to centrally collect and monitor power consumption data

across the datacenter. Now that power consumption is measurable, it becomes an actionable metric for IT staff when appropriate hardware support is available.

Microsoft recommends a collaborative model between the server platform and the operating system for power metering and budgeting (the process that lets administrators set power limits, or caps, on datacenter components as small as a single server). The server platform reports information in-band to the Windows Server 2008 R2 through the use of ACPI. The WMI namespace additions for power meters and supplies mean that the user mode power service can provide data to the WMI namespace, and this means power data can be queried by Microsoft System Center and other management tools to budget and monitor power usage across the entire IT environment. An administrator can set power budgets for the servers and the system, and can configure the system so that it automatically takes action when the budget is exceeded.

Another set of metrics can be used for virtualization and consolidation. Based on the information gathered, the workloads of underutilized servers can be consolidated onto a smaller number of better-utilized physical machines using live migration (the ability to move virtual machines between servers with virtually no downtime) with Hyper-V™. Fewer physical machines can lead to reduced costs through lower hardware and energy costs and through reduced management overhead.

New Additional Qualifier for the Designed for Windows Server 2008 R2 Logo Program

To help identify servers that have power-saving hardware capabilities, Microsoft has introduced an additional qualification for enhanced power management, the Enhanced Power Management Additional Qualifier (AQ) for the Windows Server logo.

The Windows Server Logo Program provides a way for OEMs, along with Microsoft, to help customers identify Windows-compatible products that are designed for ease of use, better performance, and enhanced security.

The Enhanced Power Management AQ ensures that power-saving features such as PPM, power metering and budgeting, and power on/power off via WS-Management (known as SMASH) capabilities are present on a server. Customers who want assurance that the hardware they are purchasing supports the additional power-saving features can look for the Enhanced Power Management AQ.

Remote Administration

Remote administration of server computers is essential to any efficient data center. It is very rare that server computers are administered locally. Windows Server 2008 R2 has a number of improvements in remote administration, including the following:

- **Remote management through graphical management consoles**. Server Manager has been updated to allow remote administration of servers. In addition, many of the management consoles have improved integration with Server Manager and as a result, support remote management scenarios. For more detailed information about each management console, see "Management Console Improvements" later in this guide.
- **Improved remote management from command-line and automated scripts**. Windows PowerShell version 2.0 has a number of improvements for remote management scenarios. These improvements allow you to run scripts on one or more remote computers or allow multiple IT professionals to simultaneously run scripts on a single computer. For more detailed information about these remote management scenarios, see "Enhanced Remote PowerShell Scenarios" later in this guide.

Reduced Administrative Effort for Interactive Administrative Tasks

Many of the management consoles used to manage Windows Server 2008 R2 have been updated or completely redesigned to help reduce administrative effort. Some of the prominent updated and redesigned management consoles are listed in the following table with a description of the improvements.

Table 2: Updated or Redesigned Management Consoles in Windows Server 2008 R2

Management console	Improvements
Server Manager	• Provides support for remote management for computers. • Improves integration with many role and role services management console.
Active Directory Administrative Center	• Based on administrative capabilities provided by Windows PowerShell cmdlets. • Task driven user interface.
Internet Information Service	• Based on administrative capabilities provided by Windows PowerShell cmdlets. • Task driven user interface.
Hyper-V Management Console	• Improved tools for day-to-day tasks • Tight integration with System Center Virtual Machine Manager for managing multiple Hyper-V servers.

Command-line and Automated Management

The Windows PowerShell version 1.0 scripting environment was shipped with Windows Server 2008. Windows Server 2008 R2 includes Windows PowerShell version 2.0, which has a number of improvements over version 1.0, including the following:

- Improved remote management
- Improved security for management data including state and configuration information
- Enhanced graphical user interfaces for creating Windows PowerShell scripts, debugging them, and viewing Windows PowerShell script output
- Extended scripting functionality supports the creation of more powerful scripts with less development effort.
- Improved portability of Windows PowerShell scripts and cmdlets between multiple computers.

Remote Management

One of the key benefits in Windows PowerShell version 2.0 is the ability to run scripts remotely with remote management by using the *PowerShell Remoting* feature. PowerShell Remoting allows you to automate many repetitive administrative tasks and then run those tasks on multiple computers. Running remote scripts is now implicit in Windows PowerShell version 2.0.

Windows PowerShell Remote Management Requirements

The PowerShell Remoting feature relies on Windows Remote Management (WS-Management) service. In order for PowerShell Remoting to work, the WS-Management service must be installed and running on the remote computer. You can verify that the WS-Management service is running by running the following Windows PowerShell cmdlet:

```
PS> get-service winrm
```

You can configure the Windows Remote Management (WS-Management) service settings, by running the following Windows PowerShell script:

```
& $pshome\Configure-Wsman.ps1
```

Note: This script does not start or stop the WS-Management service. So you will need to restart the WS-Management service for the configuration settings to take effect.

Windows PowerShell Remote Management Scenarios

Windows PowerShell version 2.0 supports the following remote management scenarios:

- **Many IT professionals running scripts on a single computer**. This scenario is also known as the *fan-in scenario*. In this scenario, each IT professional could have a customized level of access based on their credentials.
- **One IT professional running scripts on multiple computers from a single console**. This scenario is also known as the *fan-out scenario*. In this scenario, the IT professional could have different levels of access based on their credentials.
- **One IT professional interactively running scripts on a single remote computer**. This scenario is also known as the *one-to-one scenario*.
- **Run PowerShell scripts as a background job**. This scenario allows you to run a Windows PowerShell command or expression asynchronously (in the background) without interacting with the console. The command prompt returns immediately and you can query for the job results interactively. You can run background jobs on a local or remote computer.

Improved Security for Management Data

You can limit the access to management data and the ability to run commands, scripts, and other language elements by using *Constrained Runspaces*. Constrained Runspaces allow creation of Windows PowerShell Runspaces with a set of Constraints. Constraints allow you to specify the restrictions for each PowerShell Runspace.

Constrained Runspaces allow you to grant lower privileged IT professionals, such as tier 1 or tier 2 help desk personnel, the ability to examine operational state or configuration but not change operational state or configuration.

Enhanced Graphical User Interfaces

Another key improvement in Windows PowerShell version 2.0 is the new graphical user interfaces. These graphical user interfaces allow you to:

- Create and debug Windows PowerShell scripts by using Graphical PowerShell.
- View Windows PowerShell script output by using the Out-GridView cmdlet.

Create and Debug PowerShell Scripts with Graphical PowerShell

Graphical PowerShell provides a graphical user interface that allows you to interactively create and debug Windows PowerShell scripts within an integrated development environment similar to Visual Studio®.

Graphical PowerShell includes the following features:

- Syntax coloring for Windows PowerShell scripts (similar to syntax coloring in Visual Studio)
- Support for Unicode characters
- Support for composing and debugging multiple Windows PowerShell scripts in a multi-tabbed interface
- Ability to run an entire script, or a portion a script, within the integrated development environment
- Support for up to eight PowerShell Runspaces within the integrated development environment

Note: Graphical PowerShell feature requires Microsoft .NET Framework 3.0.

View Windows PowerShell Scripts Output with Out-GridView Cmdlet

The new Out-GridView cmdlet displays the results of other commands in an interactive table, where you can search, sort, and group the results. For example, you can send the results of a

get-process, get-wmiobject, or get-eventlog command to out-gridview and use the table features to examine the data.

Note: Out-gridview cmdlet feature requires Microsoft .NET Framework 3.0.

Extended Scripting Functionality

Windows PowerShell 2.0 includes the ability to extend PowerShell scripts functionality by using the following features:

- **Create advanced functions**. Advanced functions allow you to write wrappers around existing cmdlets. Windows PowerShell 2.0 searches for functions first and then cmdlets. This allows advanced functions to take precedence over cmdlets.
- **Call .NET application programming interfaces (APIs)**. This feature allows you to extend your Windows PowerShell with the features provided by any .NET API.
- **Improved script debugging**. Windows PowerShell 2.0 allows you to set breakpoints on lines, columns, functions, variables, and commands. You can also specify actions to run when the breakpoint is hit. The debugging environment supports stepping into, over, or out of functions. You can also get the call stack information (breakpoints).
- **Subscription-based interface to Windows Event System**. This feature allows your Windows PowerShell scripts to respond to specific events in event logs.
- **Write cmdlets in PowerShell script**. This feature allows you to write cmdlets in Windows PowerShell instead of compiled C# or VB.NET.
- **Script Internationalization**. This new feature allows Windows PowerShell script authors to write scripts that can be translated to any language supported by Windows.
- **New and updated cmdlets**. Windows PowerShell 2.0 includes over 240 new cmdlets out of the box. Get more information on these at the PowerShell Community Web site.

Portability of Windows PowerShell Scripts and Cmdlets

Another area of improvement for Windows PowerShell 2.0 is in the area of portability. The improved portability in Windows PowerShell 2.0 allows you to easily move PowerShell scripts and cmdlets between computers.

The features that help improve the portability of Windows PowerShell scripts and cmdlets include:

- **New module architecture**. This architecture allows the packaging of cmdlets, which includes the definition and packaging of scripts. You can send these packaged modules to other administrators.

- **New method of storing configuration information**. In Windows PowerShell version 1.0 some of the configuration was put in the registry. In Windows PowerShell version 2.0 the configuration is stored in an .xml file. The .xml file allows the configuration information to be more easily moved from one computer to another.

  Note: Although you must uninstall PowerShell 1.0 before installing Windows PowerShell 2.0, the registry settings are automatically migrated to the .xml file.

Improved Identity Management

Identity management has always been one of the critical management tasks for Windows-based networks. The implications of a poorly managed identity management system are one of the largest security concerns for any organization.

Windows Server 2008 R2 includes identity management improvements in the Active Directory Domain Services and Active Directory Federated Services server roles.

Improvements for All Active Directory Server Roles

Windows Server 2008 R2 includes the following identity management improvements that affect all Active Directory server roles:

- **New forest functional level**. Windows Server 2008 R2 includes a new Active Directory forest functional level. Many of the new features in the Active Directory server roles require the Active Directory forest to be configured with this new functional level.
- **Enhanced command line and automated management**. Windows PowerShell cmdlets provide the ability to fully manage Active Directory server roles. The Windows PowerShell cmdlets augment the graphical management tools and help automate repetitive management tasks.

Improvements in Active Directory Domain Services

The Active Directory Domain Service server role in Windows Server 2008 R2 includes the following improvements:

- **Recovery of deleted objects**. Active Directory domains now have a Recycle Bin feature that allows you to recover deleted objects. If an Active Directory object is inadvertently deleted, you can restore the object from the Recycle Bin.
- **Improved process for joining domains**. Computers can now join a domain without being connected to the domain during the deployment process, also known as an *offline domain join*. This process allows you to fully automate the joining of a domain during

deployment. Domain administrators create a file that can be included as a part of the automated deployment process. The file includes all the information necessary for the target computer to join the domain.

- **Improved management of user accounts used as identity for services**. One of the time consuming management tasks is to maintain passwords for user accounts that are used as identities for services, also known as *service accounts*. When the password for a service account changes, the services using that identity must also be updated with the new password. To address this problem, Windows Server 2008 R2 includes a new feature called *managed service accounts*. In Windows Server 2008 R2, when the password for a service account changes, the managed service account feature automatically updates the password for all the services that use the service account.
- **Reduced effort to perform common administrative tasks**. Windows Server 2008 R2 includes a new Active Directory Domain Services management console, Active Directory Administrative Center (as illustrated in the following figure).

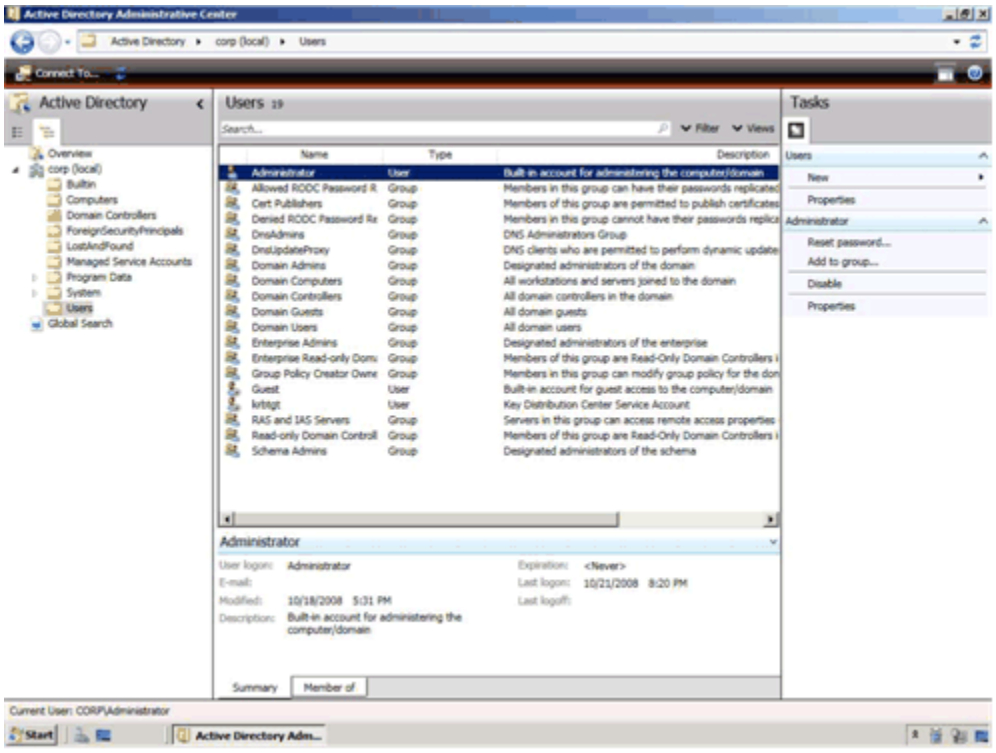

Figure 11: Active Directory Administrative Center management console

Active Directory Administrative Center is a task-based management console that is based on the new Windows PowerShell cmdlets in Windows Server 2008 R2.

Active Directory Administrative Center is designed to help reduce the administrative effort for performing common administrative tasks.

Improvements in Active Directory Federated Services

Active Directory Federated Services in Windows Server 2008 R2 includes a new feature called *authentication assurance*. Authentication assurance allows you to establish authentication policies for accounts that are authenticated in federated domains. For example, you might require smart card authentication, or other biometric authentication, for any users in federated domains.

Improved Compliance with Established Standards and Best Practices

Windows Server 2008 R2 includes an integrated Best Practices Analyzer for each of the server roles. You can run the Best Practices Analyzer to provide you with a set of configuration recommendations for the server role. The Best Practices Analyzer creates a checklist within Server Manager for the role that you can use to help you perform all the configuration tasks. The following figure illustrates a sample of the recommendations from the Best Practices Analyzer for the Active Directory Domain Services server role.

Web

Windows Server® 2008 R2 includes many enhancements that make this release the most robust Windows Server Web application platform yet. It offers an updated Web server role – Internet Information Services (IIS) 7.5– and greater support for .NET on Server Core. Design goals for IIS 7.5 concentrated on improvements that enable Web administrators to more easily deploy and manage Web applications, and that increase both reliability and scalability. Additionally, IIS 7.5 has streamlined management capabilities and provides more ways than ever to customize your Web serving environment.

Reduced Effort to Administer and Support Web-based Applications

Reducing the effort required to administer and support Web-based applications is a key differentiator for IIS 7.5. Included with this release is support for increased automation, new remote administration scenarios, and improved content publishing for developers and authors. A short list of these features includes:

- Expanding the capabilities of IIS Manager through new management modules;
- Automating common administrative tasks through the Windows PowerShell™ Provider for IIS;
- Support for .NET on Server Core, enabling ASP.NET and remote management through IIS Manager.

Automation of Common Tasks Through the PowerShell Provider

The Windows PowerShell Provider for IIS is a Windows PowerShell snap-in that allows you to perform IIS administrative tasks, and manage IIS configuration and run-time data. In addition, a collection of task-oriented cmdlets provide a simple way to manage Web sites, Web applications and Web servers.

Using Windows PowerShell allows administrators to take advantage of several important features:

- Simplifying the administration by scripting common management tasks;
- Executing repetitive tasks automatically;
- Consolidating key Web metrics from all Web servers in real-time.

On a more granular level, the IIS-specific cmdlets included with Windows Server 2008 R2 ease the administrative burden for many low-level day-to-day tasks. For example, these cmdlets allow administrators to add and change configuration properties of Web sites and Web-based applications as well as virtual directories and application pools. Users more familiar with Windows PowerShell will be able to execute advanced configuration tasks and even integrate existing Windows PowerShell scripts with other Windows PowerShell providers across different Windows Server 2008 R2 feature areas. A few common scenarios for Windows PowerShell within IIS 7.5 management might include:

- Adding/modifying/deleting sites and applications;
- Migrating site settings;
- Configuring SSL and other security settings;

- Restricting access by IP address;
- Backing up IIS configuration and content.

Enhancements to IIS Manager

New features have been added to IIS Manager for the 7.5 release that make it possible to manage obscure settings such as those used for FastCGI and ASP.NET applications or adding and editing request filtering rules through a graphical user interface.

Configuration Editor

Configuration Editor (illustrated in the following figure) allows you to manage any configuration section available in the configuration system. Configuration Editor exposes several configuration settings that are not exposed elsewhere in IIS Manager.

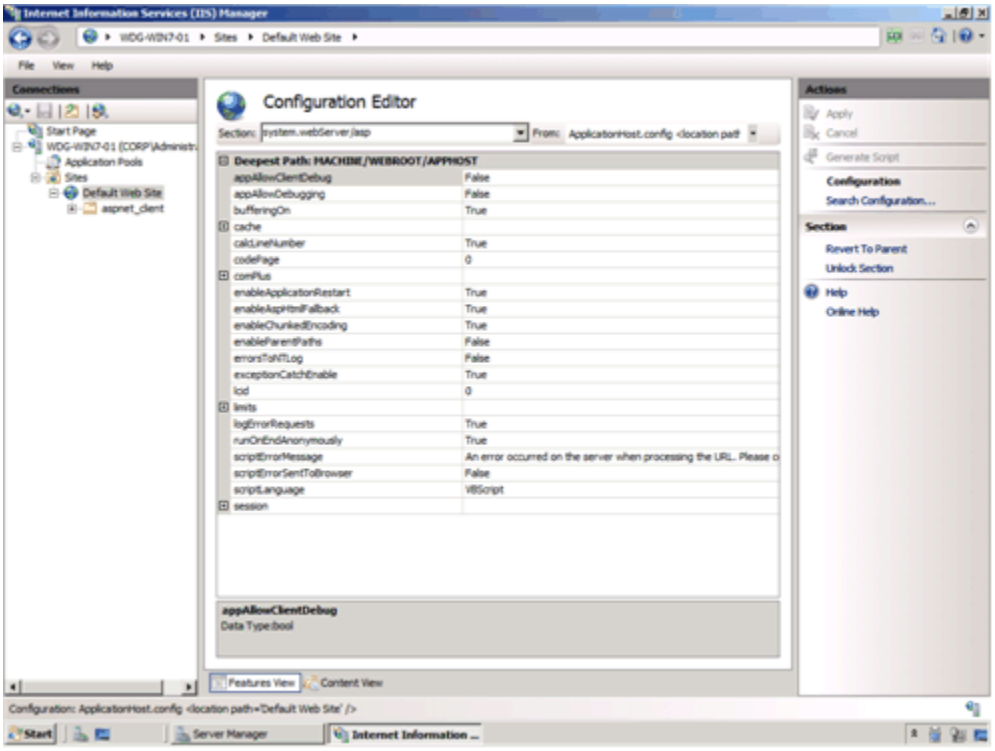

Figure 12: Configuration Editor user interface

IIS Manager UI Extensions

Utilizing the extensible and modular architecture introduced with IIS 7.0, the new IIS 7.5 integrates and enhances existing extensions and allows for further enhancements and customizations in the future. The FastCGI module, for example, allows management of

FastCGI settings while the ASP.NET module allows management of authorization and custom error settings.

Request Filtering

The Request Filter module in Windows Server 2008 R2 will include the filtering features previously found in URLScan 3.1. By blocking specific HTTP requests, the Request Filter module helps prevent potentially harmful requests from being processed by Web applications on the server. The Request Filtering user interface (illustrated in the following figure) provides a graphical user interface for configuring the Request Filtering module.

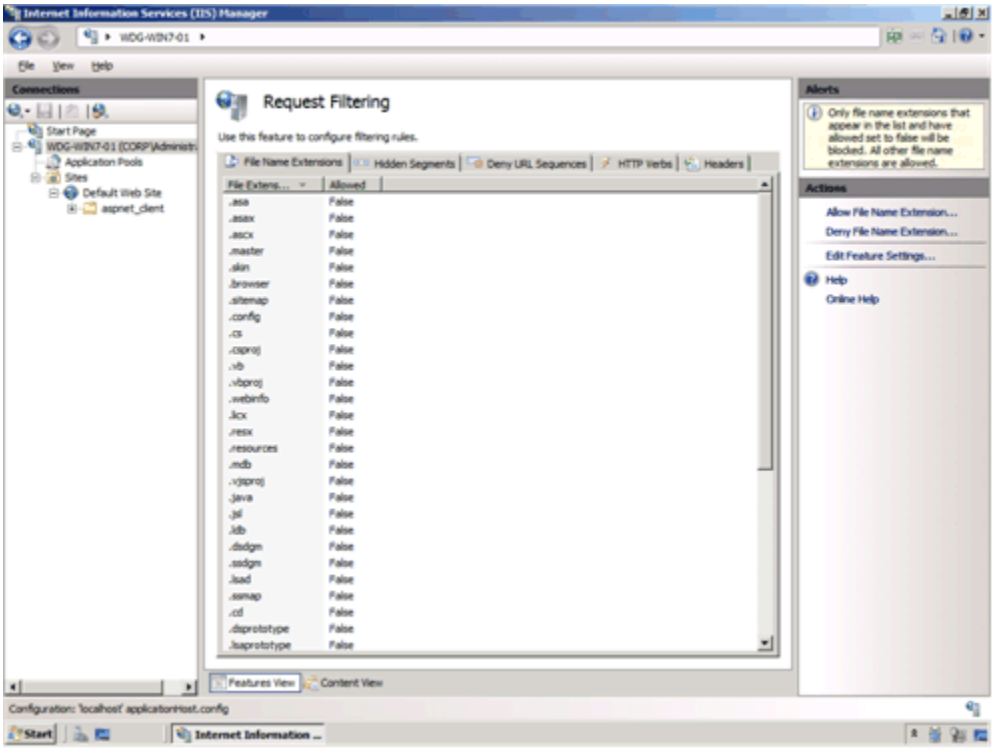

Figure 13: Request Filtering user interface

Managed Service Accounts

Windows Server 2008 R2 allows domain-based service accounts to have passwords that are managed by Active Directory® Domain Services (AD DS). These new type of accounts reduce the recurrent administrative task of having to update passwords on processes running with these accounts. IIS 7.5 supports the use of managed service accounts for application pool identities.

Hostable Web Core

Developers are able to service HTTP requests directly in their applications by using the hostable Web core feature. Available through a set of APIs, this feature lets the core IIS Web engine to be consumed or hosted by other applications, allowing those apps to service HTTP requests directly. The hostable Web core feature is useful for enabling basic Web server capabilities for custom applications or for debugging applications.

Reduced Support and Troubleshooting Effort

Windows Server 2008 R2 reduces support and troubleshooting effort in the following ways:

- **Enhanced auditing of changes to IIS 7.5 and application configuration**. The new Configuration Logging feature in IIS 7.5 provides enhanced auditing of changes to IIS and application configuration, which allows you to track the configuration changes made to your test and production environments. This provides logging of both reads and writes as well as logon attempts, changes to path mappings, file creations and more.

- **Failed Request Tracing for FastCGI**. In IIS 7.5, PHP developers can use the FastCGI module to include IIS trace calls in their applications. This reduces the effort required for debugging code during development and troubleshooting application errors after deployment by using IIS Failed Request Tracing.

- **Best Practices Analyzer (BPA)**. The BPA for IIS 7.5 is a management tool that can help you reduce best practice violations by scanning an IIS 7.5 Web server and reporting on potential configuration issues found. You can access the BPA through Server Manager and Windows PowerShell.

Improved FTP Services

Windows Server 2008 R2 includes a new version of FTP Server services. These new FTP server services offer the following improvements:

- **Reduced administrative effort for FTP server services**. The new FTP server is fully integrated with the IIS 7.5 administration interface and configuration store, as shown in the following figure. This allows administrators to perform common administrative tasks within one common administration console.

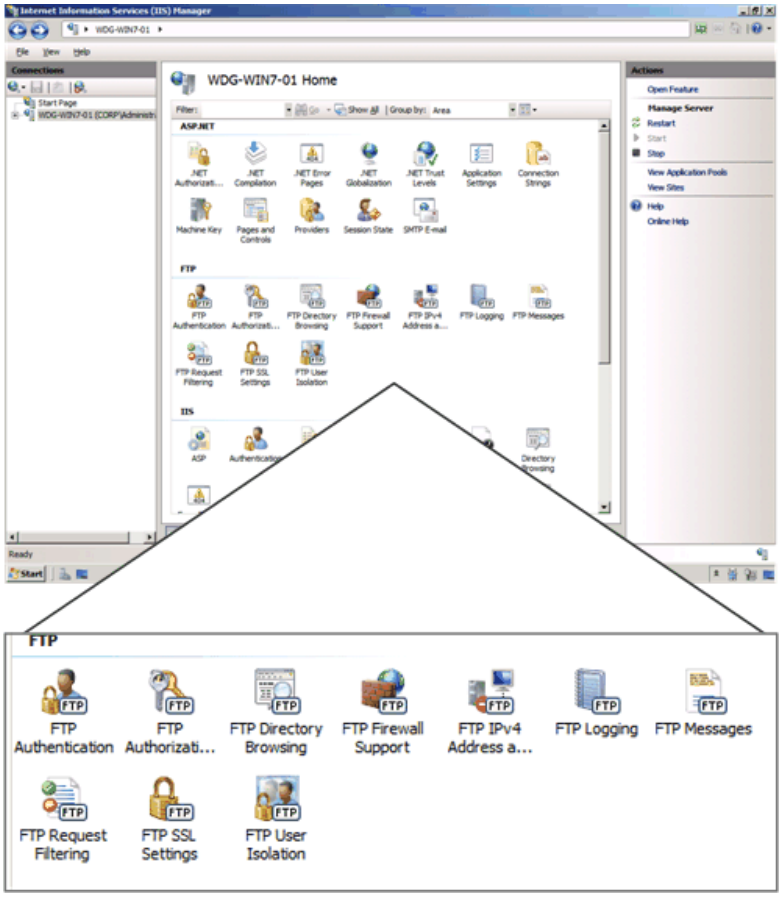

Figure 14: Integration of the FTP server administration in Internet Information Service Manager

- **Extended support for new Internet standards**. The new FTP server includes support for emerging standards, including:
  - Improved security by supporting FTP over secure sockets layer (SSL);

- Support of extended character sets by including UTF8 support;
- Extended IP addressing features provided by IPv6.

- **Improved integration with web-based applications and services**. With the new FTP server, you can specify a, virtual host name for an FTP site. This allows you to create multiple FTP sites that use the same IP address, but are differentiated by using unique virtual host names. This allows you to provide FTP and Web content from the same Web site simply by binding an FTP site to a Web site.
- **Reduced effort for support and troubleshooting FTP–related issues**. Improved logging that now supports all FTP-related traffic, unique tracking for FTP sessions, FTP sub statuses, an additional detail field in FTP logs, and more.

Ability to Extend Functionality and Features

One of the design goals for IIS 7.5 was to make it easy for you to extend the base functionality and features in IIS 7.5 IIS Extensions allow you to build or buy software that can be integrated into IIS 7.5 in such a way that the software appears to be an integral part of IIS 7.5. The following figure illustrates the placement of IIS Extensions in the IIS 7.5 architecture.

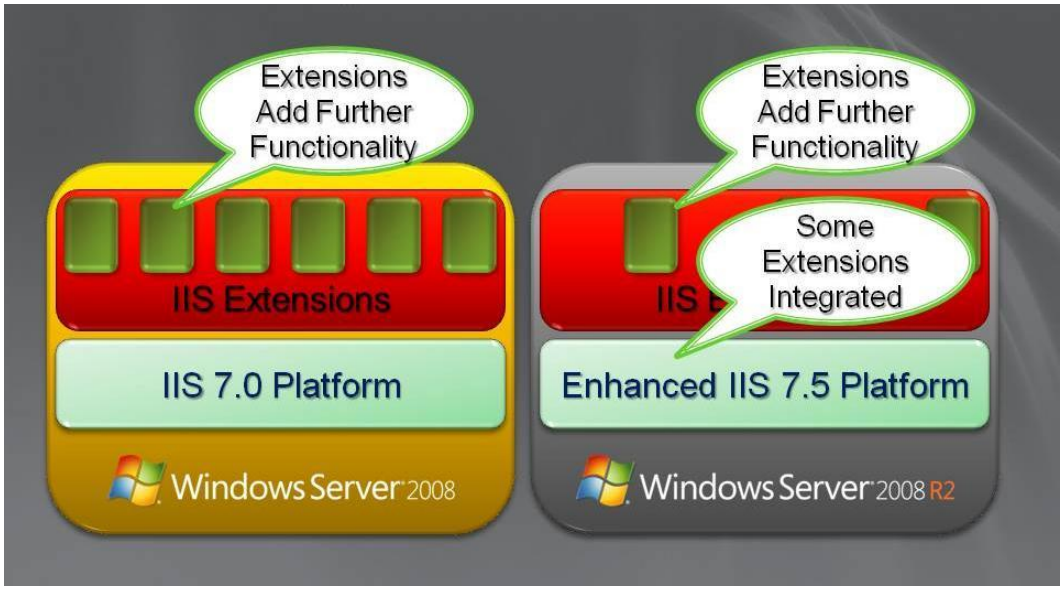

Figure 15: Architecture of IIS Extensions in IIS 7.5 in Windows Server 2008 R2

Extensions can be created by Microsoft, partners, independent software vendors, and your organization. Microsoft has developed IIS Extensions since the RTM version of Windows Server 2008. These IIS Extensions are available for download from

http://www.iis.net/extensions. Many of the IIS Extensions developed by Microsoft will be shipped as a part of Windows Server 2008 R2, including:

- IIS WebDAV;
- Integrated and enhanced Administration Pack;
- Windows PowerShell Snap-In for IIS.

Improved .NET Support

The .NET Framework (versions 2.0, 3.0, 3.5.1 and 4.0) is now available on Server Core as an installation option. By taking advantage of this feature, administrators can enable ASP.NET on Server Core which affords them full use of Windows PowerShell cmdlets. Additionally, .NET support means the ability to perform remote management tasks from IIS manager and host ASP.NET Web applications on Server Core as well.

Improved Application Pool Security

Building on the application pool isolation that was available with IIS 7.0 that increased security and reliability, every IIS 7.5 application pool now runs with a unique, less-privileged identity. This helps harden the security of applications and services running on IIS 7.5.

IIS.NET Community Portal

To stay current with new additions to IIS in Windows Server 2008 or Windows Server 2008 R2, make sure to visit the IIS.NET community portal (http://www.iis.net). The site includes update news, in-depth instructional articles, a download center for new IIS solutions and free advice via blogs and technical forums.

Solid Foundation for Enterprise Workloads

Windows Server® 2008 R2 has been designed as an enterprise-class operating system, capable of scaling to the largest data center workloads, while helping to ensure strong security and high-availability. Windows Server 2008 R2 allows you to create solutions that can solve your most demanding technical requirements. Specifically, Windows Server 2008 R2 provides enterprise-class foundation for workloads by providing:

- Improved scaling, reliability, and security for all your solutions.
- A platform with future growth potential that will allow you to take advantage of future operating systems, such as Windows® 7.

Improved Scalability, Reliability, and Security

Every application is mission critical to the users that depend on the application for performing their day-to-day job functions. Any outages of services, slow performance, or compromise in security results in loss in productivity and potential damage to your organization.

Windows Server 2008 R2 helps you create solutions that are able to support your mission critical applications, while helping to also ensure that you can manage your solutions with less effort than with previous operating system platforms.

Windows Server 2008 R2 helps improve the scalability, reliability, and security of your solutions with the following features:

- Increased processor performance and memory capacity for applications.
- Improved application platform security for all applications running on Windows Server 2008 R2.
- Improved availability and scalability for applications and services.
- Improved security for Domain Name System (DNS) services by using the DNSSEC feature.

Increased Processor Performance and Memory Capacity

The improvements in computer design have resulted in modern server computers that support ever increasing number of processors and increased memory capacity. Current

server computers are only shipping with 64-bit processors, with multiple processors, and higher memory capacity than ever before.

These improvements allow you to create application platforms that are able to support larger workloads, reduce rack space in your data center, reduce power consumption, provide improved reliability, and reduce your overall administrative effort.

Improved Physical Processor and Memory Resources

32-bit processors impose system resource limitations that restrict your ability to handle increased workloads without investing in additional server computers. 64-bit processors allow you to support larger workloads, while minimizing the number of physical computers in your data center. Also, server consolidation by using virtualization requires 64-bit processors to provide the processing and memory resources to support higher ratios of server consolidation.

To support the increased processor performance and memory capacity provided by 64-bit processors, Windows Server 2008 R2 is only available for 64-bit processor architectures. Windows Server 2008 R2 supports up to 256 logical processor cores for a single operating system instance.

Increased Logical Processor Support

Windows Server 2008 R2 Hyper-V™ supports up to 64 logical processors.. This increased processor support makes it possible to run even more demanding workloads on a single computer, or scale workloads to greater extremes to match changing demand.

Windows Server 2008 R2 Hyper-V also supports Second-Level Address Translation (SLAT) and CPU Core Parking. SLAT uses special processor functionality available in recent Intel and AMD processors to carry out some virtual machine memory management functions, significantly reducing hypervisor processor time and saving about 1MB of memory per virtual machine. CPU Core Parking enables power savings by scheduling virtual machine execution on only some processor cores and placing the remaining processor cores in a sleep state.

Improved Application Platform Security

Windows Server operating systems have included the concept of server roles for a number of versions. Windows Server 2008 R2 includes even more granular definition of server roles than in previous Windows Server operating systems. This finer granularity allows you to install only the operating system components and features that you need to support your applications and services, which reduces the attack surface of your solution.

In addition, the Windows Server 2008 R2 Server Core installation option now supports more server roles, such as .NET application support, than in Windows Server 2008 RTM. The Server Core installation option further reduces the attack surface of your solution by eliminating the graphical user interface on Windows Server 2008. Additional management features for the Server Core installation option, such as improvements in Windows PowerShell™ v2.0 and PowerShell Remoting, help reduce the administrative effort for supporting solutions with the Server Core installation option.

Availability and Scalability for Applications and Services

Availability is a key element in every solution in your enterprise. Today most mission critical applications are running on Windows Server and those applications require high availability. Failover clustering in Windows Server 2008 R2 has many improvements that can help overall application and operating system availability, including the following:

- **Enhanced cluster validation tool**. Windows Server 2008 R2 includes a best practice analyzer test which examines the best practices configuration settings for a cluster and cluster nodes. The test runs only on computers that are currently cluster nodes.
- **Enhanced command line and automated management**. Windows PowerShell cmdlets provide the ability to fully manage failover clusters and the applications running on the cluster. The Windows PowerShell cmdlets replace cluster.exe, which provided a command-line and scriptable interface for managing failover clusters in previous versions of Windows Server.
- **Improved performance for intermittent or slow secured network connections.** There are improvements in Internet Protocol security (IPsec) reconnection time that is achieved by eliminating some of the initial handshaking when reconnecting due to intermittent or slow connections.
- **Improved network resiliency between cluster nodes**. The connectivity between cluster nodes has been revised to give clusters the ability to recover from intermittent or slow connections between cluster nodes without affecting cluster node status.
- **Improving the monitoring of clusters, cluster nodes, and applications**. Failover clustering in Windows Server 2008 R2 includes the following improvements that help in failover cluster monitoring:
    - New performance counters that help reduce the support and troubleshooting effort for cluster-based applications.
    - New logging channel that helps clearly identify failover clustering-related events.
    - New support issue solutions that can be accessed directly while viewing the events for the top support issues.

- **Secure access to cluster monitoring and configuration information**. The failover clustering Windows PowerShell provider leverages the delegated permissions available in PowerShell 2.0 to provide read-only access to cluster monitoring and configuration information. This allows you to allow less privileged IT professionals read-only access, while allowing high privileged IT professionals read and write access. For more information on delegate permissions in Windows PowerShell 2.0, see "Improved Security for Management Data" in "Management" earlier in this guide.
- **Improved migration of supported cluster workloads**. You can migrate cluster workloads currently running on Windows Server 2003 and Windows Server 2008 to Windows Server 2008 R2. The migration process supports:
  - Every workload currently supported on Windows Server 2003 and Windows Server 2008, including Distributed File System Namespace (DFS-N), Dynamic Host Configuration Protocol (DHCP), DTC, File Server, Generic Application, Generic Script, Generic Service, Internet Storage Name Service (iSNS), Network File System (NFS), Other Server, Remote Desktop Session Broker, and Windows Internet Naming Service (WINS).
  - Supports most common network configuration.
  - Does not support rolling upgrades of clusters (cluster workloads must be migrated to a new cluster running Windows Server 2008 R2).
- **Includes new high availability roles for failover clustering**. Failover clustering in Windows Server 2008 R2 includes new high availability roles, including DFS-Replication, Hyper-V, and Terminal Services Session Broker.
- **Improvements in cluster node connectivity fault tolerance**. If a cluster node loses:
  - Connectivity to a shared disk, the cluster node can write to the shared disk through other cluster nodes (also known as dynamic I/O redirection).
  - Network connectivity through the primary network adapter, the cluster node can access the network through the primary network adapter of other cluster nodes.
- **Improvements for virtual machine management**. The Live Migration feature in Hyper-V version 2.0 allows virtual machines to be moved between failover cluster nodes without interruption of services provided by the virtual machines. The Live Migration feature requires shared disk storage between the cluster nodes. The shared disk storage can be provided by any vendor-based solution or by the new Cluster Shared Volumes feature in failover clustering. The Cluster Shared Volumes feature supports a file system that is shared between cluster nodes. This feature is implemented as a filter driver in Windows Server 2008 R2. It is manually enabled by configuring a cluster wide property in Windows PowerShell (%{$_.EnableSharedVolumes=1}). It is not supported with cluster

nodes in multiple sites. This feature leverages other failover cluster features, such as dynamic I/O redirection to maintain connectivity to disks. The Cluster Shared Volumes feature has no:

- Special hardware requirements.
- Special application requirements.
- File type restrictions.
- Directory structure or depth limitations.
- Special agents or additional installations.
- Proprietary file system (uses NTFS).

For more information on the Live Migration feature, see "Improved Management of Virtual Datacenters" in "Virtualization" earlier in this guide.

Improved Performance and Scalability for Applications and Services

Another key design goal was to provide higher performance for Windows Server 2008 R2 running on the same system resources as previous versions of Windows Server. In addition, Windows Server 2008 R2 supports increased scaling capabilities that allow you to support greater workloads than ever before. The Windows Server 2008 R2 features that improve performance and scalability for applications and services include:

- Support for larger workloads by adding additional servers to a workload (scaling out).
- Support for larger workloads by utilizing or increasing system resources (scaling up).

Increased Workload Support by Scaling Out

The Network Load Balancing feature in Windows Server 2008 R2 allows you to combine two or more computers in to a cluster. You can use Network Load Balancing to distribute workloads across the cluster nodes to support larger number of simultaneous users. The Network Load Balancing feature improvements in Windows Server 2008 R2 include:

- Improved support for applications and services that require persistent connections.
- Enhanced command line and automated management for Network Load Balancing clusters.
- Improved health monitoring and awareness for applications and services running on Network Load Balancing clusters.

Improved Support for Applications and Services that Require Persistent Connections

The IP Stickiness feature in Network Load Balancing allows you to configure longer affinity between client and cluster nodes. By default, Network Load Balancing distributes each request to different nodes in the clusters. Some applications and services, such as a shopping cart application, require that a persistent connection is maintained with a specific cluster node.

You can configure a timeout setting for connection state to a range of hours or even weeks in length. Examples of applications and services that can utilize this feature include:

- Universal Access Gateway (UAG) that uses a Secure Sockets Layer (SSL)-based virtual private network (VPN).
- Web-based applications that maintain user information, such as an ASP.NET shopping cart application.

Enhanced Command line and Automated Management

Windows PowerShell cmdlets provide the ability to fully manage Network Load Balancing clusters and the applications running on the cluster. The Windows PowerShell cmdlets replace nlb.exe, which provided a command-line and scriptable interface for managing Network Load Balancing clusters in previous versions of Windows Server. These Windows PowerShell cmdlets allow you to:

- Create and destroy clusters.
- Add, remove, and control cluster nodes.
- Add, edit, and remove cluster virtual IP addresses and dedicated IP addresses.
- Provide support for local and remote management.

Improved Health Monitoring and Awareness for Applications and Services

The Network Load Balancing Management Pack for Windows Server 2008 R2 allows you to monitor the health of applications and services running in Network Load Balancing clusters. This allows you to identify when applications on cluster nodes or entire cluster nodes have failed and requires attention.

Increased Workload Support by Scaling Up

Windows Server 2008 R2 includes features that also allow you to support larger workloads on individual computers. Scaling up allows you to reduce the number of servers in your data center and be more power efficient. The features that support scaling up include:

- **Increased number of logical processors supported**. Windows Server 2008 R2 Datacenter Edition supports up to 256 logical processors.

- **Reduced operating system overhead for graphical user interface**. In addition to reducing the attack surface of the operating system, the Server Core installation option eliminates the graphical user interface, which reduces the amount of processor utilization. The reduction in processor utilization allows more of the processing power to be used for running workloads.
- **Improved performance for storage devices.** Windows Server 2008 R2 includes a number of performance improvements for storage devices connected locally, through Internet Small Computer System Interface (iSCSI), and other remote storage solutions. For more information on these improvements in storage device performance, see "Improved Storage Solutions" later in this section.

Improved Storage Solutions

The ability to quickly access information is more critical today than ever before. The foundation for this high-speed access is based on file services and network attached storage. Microsoft storage solutions are at the core of providing high-performance and highly-available file services and network attached storage.

The release version of Windows Server 2008 had many improvements in storage technologies. Windows Server 2008 R2 includes additional improvements that help the performance, availability, and manageability of storage solutions.

Improved Storage Solution Performance

Windows Server 2008 R2 includes a number of performance improvements in storage solutions, including:

- **Reduction in processor utilization to achieve "wire speed" storage performance**. Wire speed (or wire speed) refers to the hypothetical maximum data transmission rate of a cable or other transmission medium. Wire speed is dependent on the physical and electrical properties of the cable, combined with the lowest level of the connection protocols. Windows Server 2008 RTM is able to access storage at wire speed, but at a higher processor utilization than Windows Server 2008 R2.
- **Improved storage input and output process performance**. One the primary contributors to the storage performance improvements for Windows Server 2008 R2 is the improvement in the storage input and output process, known as NTIO. The NTIO process has been optimized to reduce the overhead in performing storage operations.

- **Improved performance when multiple paths exist between servers and storage**. When multiple paths exist to storage, you can load-balance storage operations by load-balancing the storage requests. Windows Server 2008 R2 supports up to 32 paths to storage devices, while Windows Server 2008 RTM only supported two paths. You can configure load-balancing policies to optimize the performance for your storage solution.
- **Improved connection performance for iSCSI attached storage**. The iSCSI client in Windows Server 2008 R2 has been optimized to improve the performance for iSCSI attached storage. These improvements include:
  - **Offload iSCSI digest**. This includes offloading of iSCSI initiator CRC (header and data digests) to hardware, which can result in a 20 percent reduction in processor utilization for iSCSI. The iSCSI digest offload is supported by Intel Nehalem/I7 processors.
  - **Support for NUMA IO**. This allows the processing of disk IO request to be completed on the same processor on which the request was initiated.
  - **Reduction in lock contention**. The core IO path for Windows Server 2008 R2 has been optimized to reduce contention for multiple IO threads running concurrently.
  - **Improved support for virtual machines**. Many of the same optimizations provided for Windows Server 2008 R2 running on a physical computer are available for virtual machines. These improvements affect the network interfaces and iSCSI initiators for virtual machines. This includes support for TCP Chimney, Large Send Offload (LSO) v2, and Jumbo Frames. Each of these improvements can help increase the performance for virtual machines using the iSCSI initiator.
- **Improved support for optimization of storage subsystem**. The storage system has been designed to allow hardware vendors to optimize their storage mini-driver. For example, a vendor could optimize the disk cache for their storage mini-driver.
- **Reduced length of time for operating system start**. Chkdsk is run during the operating system start when an administrator has scheduled a scan of a disk volume or when volumes are not shutdown properly. Chkdsk performance has been optimized to reduce the length of time required to start the operating system. This allows you to recover faster in the event of an abnormal shutdown of the operating system (such as a power loss).

Improved Storage Solution Availability

Availability of storage is essential to all mission critical applications in your organization. Windows Server 2008 R2 includes the following improvements to storage solution availability:

- **Improved fault tolerance between servers and storage**. When multiple paths exist between servers and storage, Windows Server 2008 R2 can failover to an alternate path if the primary path fails. You can select the failover priority by configuring the load-balancing policies for your storage solution.
- **Improved recovery from configuration errors**. An error in the configuration of the storage subsystem can negatively affect storage availability. Windows Server 2008 R2 allows you to take configuration snapshots of the storage subsystem (for example, the iSCSI configuration). In the event of a subsequent configuration failure, you can quickly restore the configuration to a previous version.

Improved Storage Solution Manageability

Management of the storage subsystem is another design goal for Windows Server 2008 R2. Some of the manageability improvements in Windows Server 2008 R2 include:

- **Automated deployment of storage subsystem configuration settings**. You can automate the storage subsystem configuration settings in Windows Server 2008 R2 by customizing the Unattend.xml file.
- **Improved monitoring of storage subsystem**. The storage subsystem in Windows Server 2008 R2 includes the following improvements that help in monitoring:
    - New performance counters that help reduce the support and troubleshooting effort for storage subsystem-related issues. Extended logging for the storage subsystem, including storage drivers.
    - Health-based monitoring of the entire storage subsystem.
- **Improved version control of storage system configuration settings**. Windows Server 2008 R2 allows you to take configuration snapshots of the storage subsystem. This allows you to perform version control of configuration settings and allows you to quickly restore to a previous version in the event of a configuration error.
- **Reduction in complexity for connecting iSCSI**. Windows Server 2008 R2 includes the ability to discover and log on to a target using the DNS name or IP address of the target. This dramatically reduces the effort required to discover and log on to iSCSI targets.
- **Reduction in iSCSI configuration effort on Server Core installation options**. There is a graphical interface for configuring iSCSI which can be started from a command line in Server Core installation options.
- **Reduction in iSCSI remote management.** You can remotely manage iSCSI by using the Windows Remote Shell or by using the Psexec. For more information on iSCSI remote management by using:

- Windows Remote Shell, see http://msdn.microsoft.com/en-us/library/aa384426(VS.85).aspx.
- Psexec, see http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx.

Improved Protection of Intranet Resources

The Network Policy Server (NPS) is a Remote Authentication Dial-In User Service (RADIUS) server and proxy and Network Access Protection (NAP) health policy server. NPS evaluates system health for NAP clients, provides RADIUS authentication, authorization, and accounting (AAA), and provides RADIUS proxy functionality.

NAP is a platform that includes both client and server components to enable fully extensible system health evaluation and authorization for a number of network access and communication technologies, including:

- Internet Protocol security (IPsec)-protected communication
- 802.1X-authenticated access for wireless and wired connections
- Remote access virtual private network (VPN) connections
- Dynamic Host Configuration Protocol (DHCP) address allocation
- Terminal Service (TS) Gateway access

The improvements to NPS in Windows Server 2008 R2 include:

- **Automated NPS SQL logging setup**. This new feature automatically configures a SQL database, required tables, and store procedure for NPS accounting data, which significantly reduces the NPS deployment effort.
- **NPS logging improvements**. The logging improvements enable NPS to simultaneously log accounting data to both a file and a SQL database, support failover from SQL database logging to file logging, and support logging with an additional file format that is structured similar to SQL logging.
- **NAP multiple configurations of a system health validator (SHV).** When you configure a health policy, you can select an SHV in a specific configuration. This allows you to specify different sets of health requirements based on a specific configuration of the SHV. For example, you can create a network policy that specifies that intranet-connected computers must have their antivirus software enabled and a different network policy that specifies that VPN-connected computers must have their anti-virus software enabled and anti-malware installed.

- **NPS templates**. NPS templates separate common RADIUS configuration elements such as RADIUS shared secrets, IP filters, RADIUS clients, and others from the configuration that is running on the server. When referenced, the NPS setting inherits the values configured in the specified template. A change in the template changes the corresponding value in all of the places in which the template is referenced. For example, a single RADIUS shared secret template can be referenced for multiple RADIUS clients and servers. When you change the RADIUS shared secret template, the change is inherited by all of the RADIUS clients and servers in which that RADIUS shared secret template is referenced. NPS template settings can easily synchronized across multiple NPS servers running Windows Server 2008 R2.
- **Migration of Windows Server 2003 Internet Authentication Service (IAS) servers**. This feature allows you to migrate the configuration settings of an IAS server running on Windows Server 2003 to an NPS server running on Windows Server 2008 R2.

Improved Management of File Services

Managing data stored on file services is usually challenging because of the sheer number of files being stored on network shared folders. Because users store files on network shared with little or no restrictions, the user storing the files is the only individual who has any knowledge of the information being stored in the file and other characteristics about the file, such as sensitivity or criticality of the information in the file.

Even with this knowledge, you cannot rely on the user to properly determine the proper classification of information, data archival schedule, and other common IT operations tasks. You need to be able to centrally categorize these files and then perform IT file operations based on the classification of the files.

The Windows File Classification Infrastructure (FCI) in Windows Server 2008 R2 provides insight into your data to help you manage your data more effectively, reduce costs, and mitigate risks. The Windows File Classification Infrastructure allows you to establish policies for classifying files and then performing common administrative tasks based on the classification.

You can use the Windows File Classification Infrastructure to identify files that:

- Contain sensitive information and are located on servers with lower security and move the files to servers with higher security.
- Contain sensitive information and encrypt those files.
- Are no longer essential and automatically remove the files from servers.
- Are not accessed frequently and move the files to slower, more affordable storage solutions.

- Require different backup schedules and backup the files accordingly.
- Require different backup solutions based on the sensitivity of the information in the files.

The Windows File Classification Infrastructure allows you to:

- Centrally define policy-based classification of the files stored in your intranet.
- Perform file management tasks based on the file classification that you define, rather than on only simple information such as the location, size, or date of the file.
- Generate reports about the types of information stored in the files in your intranet.
- Notify content owners when a file management task is going to be performed on their content.
- Create or purchase custom file management solutions based on the Windows File Classification Infrastructure.

Improved Policy-based Classification of Files

One of the key advantages to the Windows File Classification Infrastructure is the ability to centrally manage the classification of the files by establishing classification policies. This centralized approach allows you to classify user files without requiring their intervention.

You can use the Windows File Classification Infrastructure to:

- Define classification properties and values, which can be assigned to files on a per-server basis by running classification rules. Property types can include Boolean, date, numbered, ordered lists, and string values.
- Create, update, and run classification rules. Each rule assigns a single predefined property and value to files within a specified directory, based on installed classification plug-ins.
- When running a classification rule, optionally re-evaluate files that are already classified. You can choose to overwrite existing classification values, or add the value to properties that support multiple values.

Improved File Management Tasks

The Windows File Classification Infrastructure allows you to perform file management tasks based on the classifications that you define. You can use the Windows File Classification Infrastructure to help you perform common file management tasks, including:

- **Grooming of data**. You can automatically delete data by using policies based on data age or classification properties to free valuable storage space and intelligently reduce storage demand growth.

- **Custom Tasks**. Execute custom commands based on age, location or other classification categories. For example, IT administrators are able to automatically move data based on policies for either centralizing the location of sensitive data or for moving data to a less expensive storage resource.

The Windows File Classification Infrastructure allows you to automate any file management task by using the file classifications you establish for your organization.

Improved Reporting on Information Stored in Files

Most IT organizations have no easy method of providing information about the types of files that are stored and managed. Without classification of the files, there is minimal information that can be used to help identify the usage of the files, the sensitivity of the files, and other relevant information about the files.

The Windows File Classification Infrastructure allows you to generate reports in multiple formats that can provide statistical information about the files stored on each file server. You can use the reporting infrastructure to generate information that can be used by another application (such as a comma separated variable format text file that could be imported into Microsoft® Excel®).

Improved File Owner Notification of File Management Tasks

Another feature of the Windows File Classification Infrastructure that reduces your administrative effort is the ability to send notifications to content owners when an automated file management task runs. For example, when files become old enough to be automatically expired, the content owners can be notified in advance and given the opportunity to prevent the files from being archived or deleted.

You can also select the method for notification based on the type of file management task being performed. And the extensible nature of the Windows File Classification Infrastructure allows you to integrate with existing messaging systems or information portals.

Improved Development of File Management Tasks

You can extend the file management features of the Windows File Classification Infrastructure by creating your own custom file management solution or purchasing a file management solution from an independent software vendor. The architecture of the Windows File Classification Infrastructure allows the use of any supported development environments for Windows Server 2008 R2, including Windows PowerShell and VBScript.

This architecture allows you to select the level of programming sophistication required to automate your file management tasks. For example, you could write Windows PowerShell scripts to manage files based on the classifications you define for your organization.

Improvements in Backup and Recovery

Backup and recovery features are very important for the continued operation of the services and applications running on Windows Server 2008 R2. Windows Server 2008 R2 includes a number of improvements that are related to backup and recovery, including improvements in:

- The Windows Server Backup utility.
- Recovering from total failures of disk volumes by using LUN synchronization.
- Integration with System Center Data Protection Manager 2007.

Improvements in Windows Server Backup

Windows Server 2008 R2 includes a new version of the Windows Server Backup utility. This new version of Windows Server Backup allows you to:

- **Backup specific files and folders**. In Windows Server 2008 RTM you had to backup and entire volume. In Windows Server 2008 R2, you can include or exclude folders or individual files. You can also exclude files based on the file types.
- **Perform incremental backup of system state**. Previously, you could only perform a full backup of the system state by using the wbadmin.exe utility. Now you can perform incremental backups of the system state by using Windows Server Backup utility, the wbadmin.exe utility, or from a Windows PowerShell cmdlet.
- **Perform scheduled backups to volumes**. You can perform a scheduled backup to existing volumes in Windows Server 2008 R2. In Windows Server 2008, you had to dedicate an entire physical disk to the backup (the target physical disk was partitioned and a new volume was created previously).
- **Perform scheduled backups to network shared folders**. You can now perform scheduled backups to a network shared folder, which was not possible in the previous version.
- **Manage backups by using Windows PowerShell**. You can manage backup and restore tasks by using Windows PowerShell (including all PowerShell remoting scenarios). This includes the management of on-demand and scheduled backups.

Improvements in Full Volume Recovery

Windows Server 2008 R2 includes support for LUN resynchronization (also known as LUN resynch or LUN revert). LUN resynchronization creates hardware-based shadow copies that allow you to recover a volume from an existing shadow copy of the volume.

LUN resynchronization is a method for quickly restoring volumes that leverages the capabilities of storage arrays (such as SANs). This allows you to create shadow copies of entire LUNs and then restore from those shadow copies (using the inherent snapshot or copying features in the storage array). You can use LUN resynchronization to help you recover from data loss or to help quickly create duplicates of productions LUNs for use in a storage environment.

Comparison of LUN Resynchronization and Traditional Volume Shadow Copy Service

Window Server 2008 R2 LUN resynchronization support is an extension of the features provided by the Volume Shadow Copy Service in Windows Server 2008 R2. LUN resynchronization uses the same application programming interfaces (APIs) that are used by the Volume Shadow Copy Service.

The following table lists the differences between LUN resynchronization and current features in Volume Shadow Copy Service.

Table 3: Comparison of LUN Resynchronization and Traditional Volume Shadow Copy Service

LUN Resynchronization	Traditional Volume Shadow Copy Service
Recovers entire LUN (which may contain multiple volumes).	Recovers only a volume.
Performed by storage array hardware.	Performed by server computer.
Typically takes less time than restoring by using traditional Volume Shadow Copy Service.	Typically takes more time than restoring by using LUN resynchronization.

Comparison of LUN Resynchronization and LUN Swap

LUN Swap is a fast volume recovery scenario that has supported since Windows Server 2003 Service Pack 1. In LUN swap, a shadow copy version of a LUN is exchanged with the active

The following table lists the differences between LUN resynchronization and LUN Swap.

Table 4: Comparison of LUN Resynchronization and LUN Swap

LUN Resynchronization	LUN Swap
Source (shadow copy) LUN remains unmodified after the resynchronization completes.	Source (shadow copy) LUN becomes the active LUN and is modified.
Destination LUN contains the same information as the source LUN, but also any information written during the resynchronization.	Contains only the information on the source LUN.
Source LUN can be used for recovery again.	Must create another shadow copy to perform recovery.
Requires the destination LUN exists and is usable.	Destination LUN does not have to exist or can be unusable.
Source LUN can exist on slower, less expensive storage.	Source LUN must have the same performance as the production LUN.

Benefits of Performing Full Volume Recovery Using LUN Resynchronization

The benefits of LUN resynchronization include the following:

- **Perform recovery of volumes with minimal disruption of service**. After the recovery of a volume using LUN resynchronization is initiated, users can continue to access data on the volume while the synchronization is being performed. Although there may be a reduction in performance, users and applications are still able to access their data.
- **Reduce the workload while recovering volumes**. Because the hardware storage array is performing the resynchronization, the server hardware resources are only minimally affected. This allows the server to continue processing other workloads with the same performance while the LUN resynchronization process is completing.
- **Integration with existing volume recovery methods**. The APIs used to perform LUN resynchronization are the same APIs that are used to perform traditional Volume Shadow Copy Service recovery. This helps ensure that you can the same tools and processes that you are currently using for traditional Volume Shadow Copy Service recovery.

- **Compatibility with future improvements**. Because LUN resynchronization uses published, supported APIs in Windows Server 2008 R2, future versions of Windows Server will also provide support for LUN resynchronization.

Process for Performing Full Volume Recovery Using LUN Resynchronization

Before you can perform a full volume recovery using LUN synchronization, you need to have a hardware shadow copy (snapshot) of the LUN. You can make full or differential shadow copies of the LUN.

The following is the sequence of events when performing a full volume restore using LUN synchronization:

1. The source and destination LUNs are identified.
2. The LUN resynchronization is initiated between the source (shadow copy) and destination LUNs.
3. During the LUN resynchronization users are able to access the volume being accessed by the following methods:
    - For read operations, volume requests are directed to the source LUN.
    - For write operations, volume requests are directed to the destination LUN.
4. The LUN resynchronization continues by performing a block-level copy from the source (shadow copy) LUN to the destination LUN.
5. The LUN resynchronization completes and all user requests are now performed from the destination LUN.

Note: At the end of the LUN resynchronization process, the source LUN is unmodified and the destination LUN contains the same information as the source LUN plus any data that was written to the destination LUN during the LUN resynchronization process.

You can find more information about how these steps are performed by viewing the Volume Shadow Copy Service APIs on MSDN® and on the Windows Software Development Kit (SDK) for Windows 7 and Windows Server 2008 R2.

Improvements in Data Protection Manager Integration

Service Pack 1 for Microsoft System Center Data Protection Manager 2007 provides continuous data protection for Windows application and file servers using seamlessly integrated disk and tape media and includes the following expanded capabilities:

- Protection of files, configuration, and other information stored on Windows Server 2008 R2.

- Protection of Hyper-V virtualization platforms, including both Windows Server 2008 R2 Hyper-V and the Microsoft Hyper-V Server, has been added to the existing set of protected workloads.

Improved Security for DNS Services

One common issue with DNS name resolution is that clients can't tell the difference between legitimate and illegitimate DNS information and are this vulnerable to spoofing and Man in the Middle attacks.

The DNS Security Extensions (DNSSEC) feature in Windows Server 2008 R2 and Windows 7 allows the DNS servers to verify authenticity of a DNS record obtained from a signed zone, and allows clients to establish a trust relationship with the DNS server.

The DNS records in a protected DNS zone include a set of public keys that are sent as DNS resource records from the DNS server services on Windows Server 2008 R2 and Windows 7. Through the use of pre-configured Trust Anchors, the DNS server can obtain the public keys of the key pair used to sign the zone and validate the authenticity of the data obtained from the zone. This method prevents interception of DNS queries and returning of illegitimate DNS responses from an untrusted DNS server.

Better Together with Windows 7

Windows Server 2008 R2 has many features that are designed to specifically work with client computers running Windows 7, the next version of client operating systems from Microsoft. The features that are only available with running Windows 7 client computers with server computers running Windows Server 2008 R2 include:

- Simplified remote connectivity for corporate computers by using the DirectAccess feature.
- Secured remote connectivity for private and public computers by using a combination of the Remote Workspace, Presentation Virtualization, and Remote Desktop Services Gateway features.
- Improved performance for branch offices by using the Branch Caching feature.
- Improved security for branch offices by using the read-only DFS feature.
- More efficient power management by using the new power management Group Policy settings for Windows 7 clients.

- Improved virtualized presentation integration by using the new desktop and application feeds feature.
- Higher fault tolerance for connectivity between sites by using the Agile VPN feature.
- Increased protection for removable drives by using the BitLocker™ Drive Encryption (BitLocker) feature to encrypt removable drives.
- Improved prevention of data loss for mobile users by using the Offline Folders feature.

Simplified Remote Connectivity for Corporate Computers

One of the common problems facing most organizations is remote connectivity for their mobile users. One of the most common solutions for remote connectivity is for mobile users to connect by using a VPN connection. Depending on the type of VPN, users may install VPN client software on their mobile computer and then establish the VPN connection over public Internet connections.

The DirectAccess feature allows Windows 7 client computer to directly connect to intranet-based resources without the complexity of establishing a VPN connection. The remote connection to the intranet is transparently established for the user. From the user's perspective, they are unaware they are remotely connecting to intranet resources.

Overview of DirectAccess

DirectAccess clients use IPv6 to communicate with the enterprise network. DirectAccess provides IPv6 addresses and connectivity to DirectAccess clients over existing IPv4 networks by using IPv4 to IPv6 transition technologies. Some of these technologies includes Teredo, 6to4, IP-HTTPS and ISATAP. Native IPv6 connectivity is also supported if the client is assigned a native IPv6 address.

The following figure illustrates an overview of a typical DirectAccess solution.

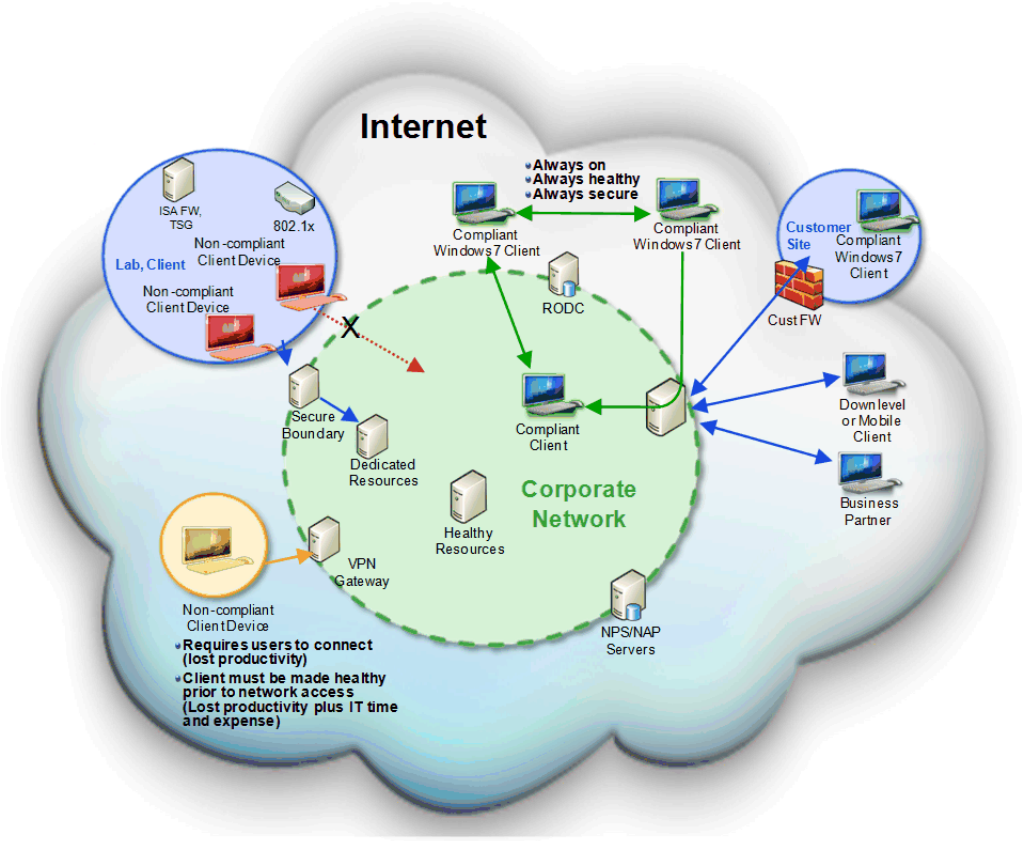

Figure 16: Overview of a typical DirectAccess solution

The components in a DirectAccess solution are listed in the following table.

Table 5: Components in a DirectAccess Solution

Component	Description
DirectAccess Client	This is a computer running Windows 7 that connects remotely to your intranet-based resources.
DirectAccess Server	This is a computer running Windows Server 2008 R2 that provides DirectAccess edge services for your organization. In addition to running DirectAccess services, this computer could also run IPv6 transition technologies as well for some deployment models.
IPv6	IPv6 is an Internet Protocol designed to solve many of the problems of the current version of IP (known as IPv4) such as address depletion, auto-configuration, and extensibility. For more information on IPv6, see www.microsoft.com/ipv6
Internet Protocol Security	Internet Protocol security (IPsec) is a framework of open standards for ensuring private, secure communications over IP networks through the use of cryptographic security services. The Internet Engineering Task Force (IETF) IPsec working group defines the IPsec standards. DirectAccess uses IPsec transport mode to secure IP traffic between the DirectAcess client and your network resources by using the authentication and encryption features in IPsec. For more information on IPsec, see www.microsoft.com/ipsec
Teredo	Teredo is an IPv6 transition technology that provides IPv6 connectivity to hosts behind a network address translation (NAT) device. For more information on Teredo, see www.microsoft.com/ipv6
6to4	6to4 is an IPv6 transition technology that provides IPv6 connectivity to hosts that have a public IPv4 address. For more information on 6to4, see www.microsoft.com/ipv6
ISATAP	ISATAP is an address assignment and automatic tunneling technology that is used to provide IPv6 connectivity between IPv6/IPv4 hosts across an IPv4 intranet. In DirectAccess, ISATAP is used to allow enterprise resources to use and route IPv6 without requiring infrastructure upgrades. For more information on ISATAP, see www.microsoft.com/ipv6
IP-HTTPS	IP-HTTPS is a new protocol for Windows 7 that allows hosts behind a proxy or firewall to establish connectivity by tunneling IP data inside of an HTTPS tunnel. HTTPS is used instead of HTTP so that proxy servers

	will not attempt to look inside of the data stream and terminate the connection if traffic looks anomalous. HTTPS is not providing security in any way; security is provided by IPsec. Since the data is double-encrypted by default (IPsec and HTTPS), IP-HTTPS may not be as performant as other protocols. Additional IP-HTTPS servers can be added and load-balanced if performance is problematic. Microsoft is looking at ways to improve the performance of this protocol in the future.
Name Resolution Policy Table	Windows 7 introduces a new feature called Name Resolution Policy Table (NRPT) is a new feature in Windows 7 that performs the following functions: • Clients can query different DNS servers for different DNS namespaces • Optionally, DNS queries for specific namespaces can be secured using IPsec (and other actions can be specified, as well) The NRPT stores a list of namespaces and configuration settings that define the DNS client's behavior specific to that namespace. Name resolution requests are matched against the namespaces stored in the NRPT and are processed according to the configuration specified. In DirectAccess, when a name resolution request matches a namespace listed in the NRPT, the NRPT settings determine whether that query will be encrypted (to protect from packet sniffing and other man-in-the-middle attacks) and which DNS servers to send that query to.

DirectAccess Connectivity Models

DirectAccess supports a number of models for connecting remote users to your intranet-based resources. These models include:

- Full Intranet Access
- Selected Server Access
- End-to-end Access

Full Intranet Access

The Full Intranet Access model, as illustrated in the following figure, allows DirectAccess clients to connect into all resources inside your intranet. This model provides IPsec-based

end-to-edge authentication and encryption which terminate at the IPsec gateway or DirectAccess™ server.

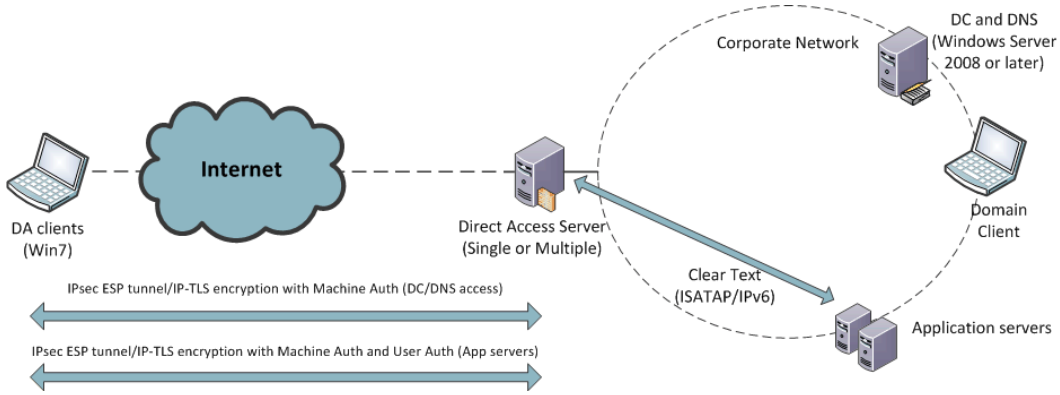

Figure 17: Full Intranet Access model

This model does not require application servers that are running Windows Server 2008 or IPsec-authenticated traffic in the enterprise network. This model most closely resembles current VPN architecture. This model is typically easier to deploy in the short term, but usually needs re-architecting long term.

The following table lists the benefits and limitations of the Full Intranet Access Model.

Table 6: Benefits and Limitations of the Full Intranet Access Model

Benefits	Limitations
Architecture similar to current VPN deployments.	Cannot secure resources based on end-to-end policies.
Does not require IPsec traffic in the enterprise network.	Might place extra load on DirectAccess Server, which can be mitigated by IPsec offload network adapters.
Works with any IPv6 capable application servers.	

Selected Server Access

The Selected Server Access model, as illustrated in the following figure, allows remote DirectAccess clients to access selected internal resources only. By leveraging IPsec, the communication between the remote client and the DirectAccess Server can be encrypted, and communication between the client and the application server can be authenticated. This allows you to define policies that restrict certain users or computers from accessing

particular application servers, or even specifying certain applications that won't be able to access intranet resources while accessing the resources remotely.

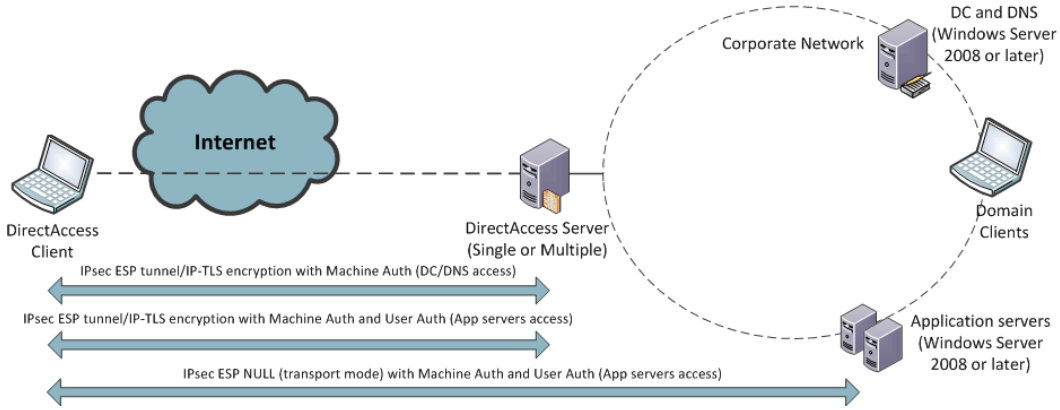

Figure 18: Selected Server Access model

The following table lists the benefits and limitations of the Selected Server Access model.

Table 7: Benefits and Limitations of the Selected Server Access Model

Benefits	Limitations
Fine grain control over which resources are available.	Application servers must be running Windows Server 2008 or later.
You can quickly realize the benefits of simplified edge policies and secure resources based on end-to-end policies.	You must be familiar with IPsec and prepared to allow this traffic inside the network.

End-to-end Access

The End-to-end Access model, as illustrated in the following figure, allows remote DirectAccess clients to access directly any intranet-based resources. The connections between the DirectAccess client, the DirectAccess Server, and the intranet-based resources are authenticated and encrypted by using IPsec, This allows you to define policies that restrict certain users or computers from accessing particular application servers, or even specifying certain applications that won't be able to access intranet resources while accessing the resources remotely.

Note: This model requires all intranet-based resources to support IPv6 and IPsec.

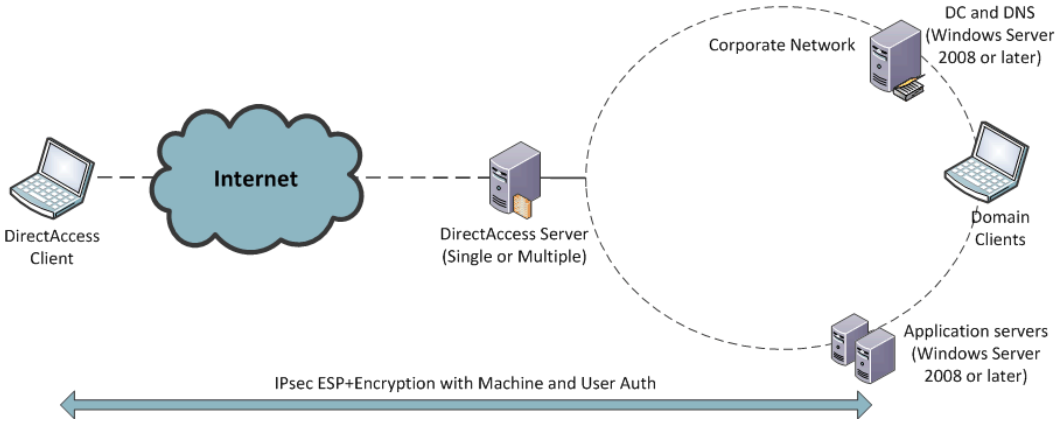

Figure 19: End to End Access Model

The following table lists the benefits and limitations of the End to End Access Model.

Table 8: Benefits and Limitations of the End to End Access Model

Benefits	Limitations
Provides end-to-end encryption of data between DirectAccess Client and intranet-based resources.	Requires IPv6 on all intranet-based resources.
No IPv6 translations services are required, which reduces the workload on DirectAccess Server(s).	Requires IPsec on all intranet-based resources

DirectAccess Requirements

Depending on the DirectAccess model selected, the requirements for deploying DirectAccess may vary. The following tables list the DirectAccess network, infrastructure, software, and hardware requirements.

Table 9: DirectAccess Network Requirements

Requirement	Description
IPv6 addressing	DirectAccess uses the IPv6 protocol to provide end-to-end connectivity between client computers and enterprise resources. This means that DirectAccess clients will have access only to those servers in your intranet that have a reachable IPv6 address. Those servers can obtain IPv6 connectivity from native IPv6 or an IPv6

	transition technology. Although IPv6 is a requirement for DirectAccess, IPv6 does not have to be enabled on network infrastructure (such as routers), only on the client and server operating systems. **Note:** A DirectAccess client can still access an Internet resource using the IPv4 protocol. IPv6 is only required when the DirectAccess client connects to your intranet resources.
IPv6 blocking	IPv6 and IPv4 protocol 41 (which is used by ISATAP and 6to4 transition technologies) must be allowed to pass through your outward facing firewalls.
Internet Protocol Security	DirectAccess uses IPsec to provide mutual authentication and encryption between the DirectAccess Client, the DirectAccess Server, and intranet-based resources (depending on the access model). Note: Only Windows Server 2008 and later server operating systems support the termination of IPsec connections over IPv6. For more information, see www.microsoft.com/ipsec.
Teredo blocking	Teredo, which uses IPv4 UDP port 3544, must be allowed to pass through your outward facing firewalls.
ICMPv6	In order for IPv6 to work properly, ICMPv6 must be allowed to pass through your outward facing firewalls.
NAT-PT devices	Network Address Translation – Protocol Translation (NAT-PT) devices can be deployed to provide DirectAccess clients access to you intranet resources that only support IPv4. NAT-PT is generally configured to provide coverage for a particular DNS namespace, and once implemented, will make the necessary translations allowing DirectAccess clients to access any IPv4 resources located within that namespace.
ISATAP	The ISATAP protocol allows direct client-to-client and client-to-server IPv6 connectivity over an IPv4 infrastructure. When DirectAccess is installed, the ISATAP server registers its name in DNS. In addition, after DirectAccess is installed all Windows-based hosts running Windows Vista® or Windows Server 2008 or later automatically obtain an ISATAP/IPv6 address from the ISATAP

	server. Since IPv6 addresses are preferred over IPv4, this means that when DirectAccess is installed, all Windows Vista, Windows Server 2008, and later operating systems in your domain will to communicate with each other using IPv6. This may have an impact on monitoring and firewall configurations.

Table 10: DirectAccess Infrastructure Requirements

Requirement	Description
Active Directory® Domain Services (AD DS)	At least one Active Directory domain is required. Workgroup-based networks and computers are not supported. At least one domain controller in the domain containing user accounts must be running Windows Server 2008 R2.
Group Policy	Group Policy can be used to deploy DirectAccess client policies and is strongly recommended.
Public Key Infrastructure	A Public Key Infrastructure (PKI) is required to issue the certificates that are required by DirectAcess and IPsec. However, external certificates (or public certificates) are not required. For more information about deploying a PKI, see http://www.microsoft.com/pki.
IPsec policies	DirectAccess uses IPsec policies, so the appropriate infrastructure must exist to manage IPsec policies. For more information, see www.microsoft.com/ipsec.
IPv6 transition technologies	ISATAP, Teredo, 6to4, and IPv6 must be available for use on the DirectAccess server.
DNS and ISATAP	DirectAccess clients query DNS for the name 'isatap' to locate ISATAP routers. DirectAccess clients also query DNS using the ISATAP protocol. In order to facilitate these requests, all DNS servers must be able to resolve the ISATAP name ('isatap') and at least some DNS servers must be listening on the ISATAP interface. You can enable these capabilities by: • Ensuring some DNS servers run Windows Server 2008 SP2 or Windows Server 2008 R2 • Unblocking ISATAP name resolution on all DNS servers

Table 11: DirectAccess Software Requirements

Requirement	Description
DirectAccess Server	DirectAccess Server is an optional component of Windows Server 2008 R2 that manages DirectAccess connections, The DirectAccess Server may either terminate or pass IPsec connections.
DirectAccess Client	DirectAccess Client is an optional component of Windows 7 that allows remote users to connect to DirectAccess Servers. **Note:** Computers running Windows Vista or earlier operating system versions do not support DirectAccess

Table 12: DirectAccess Hardware Requirements

Requirement	Description
DirectAccess Server	The hardware requirements for DirectAccess Server are the same as those for Windows Server 2008 R2. However, all DirectAccess servers must have at least two physical network adapters installed.
DirectAccess Client	The hardware requirements for DirectAccess Server are the same as those for Windows 7.

DirectAccess Firewall Placement and Rules

Because DirectAccess allows Internet-based clients access to intranet-based resources, placement of firewalls and configuration of firewall rules is important. The following figure illustrates the placement of DirectAccess components in relationship to a typical firewall configuration.

Note: The following figure does not represent a design requirement, but rather recommended best practices. Depending on your firewall configuration, placement of DirectAccess components may differ.

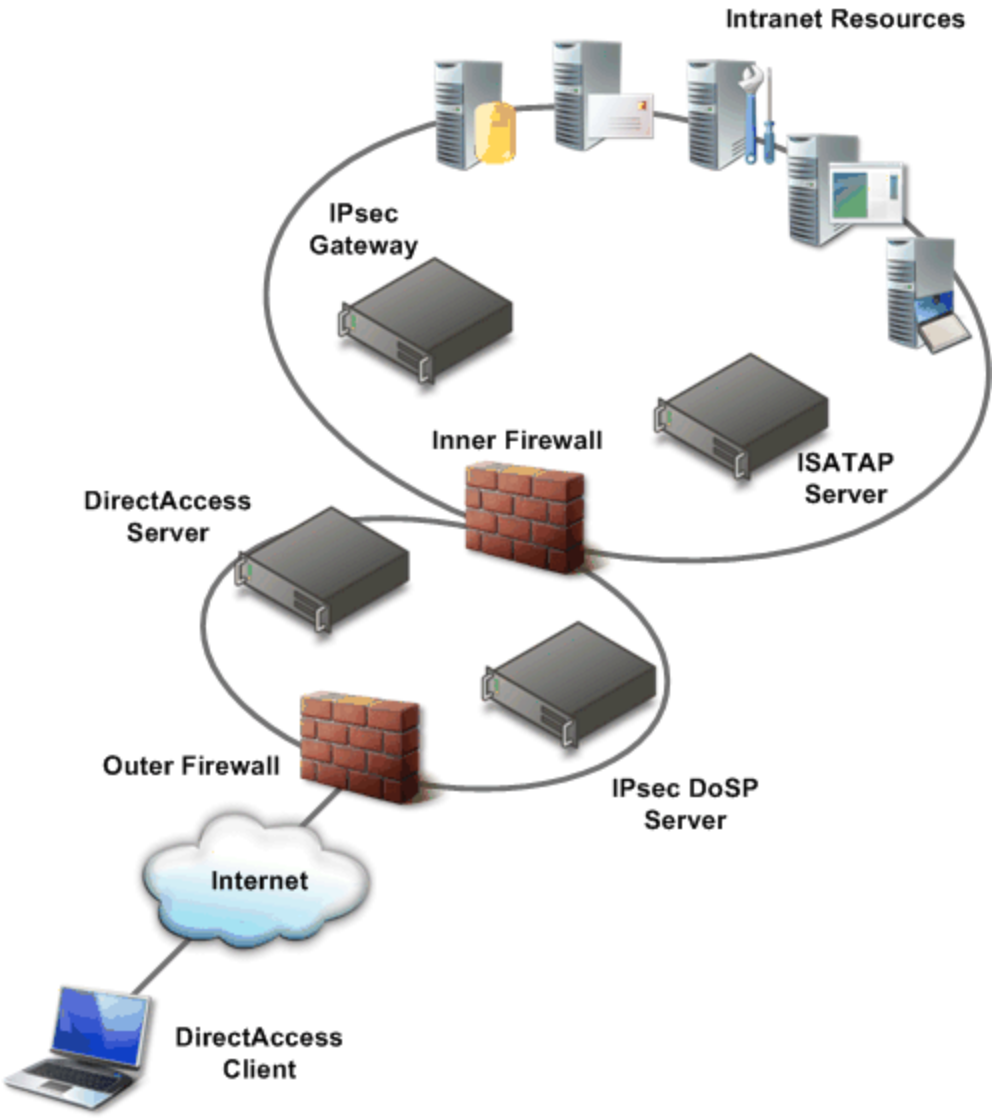

Figure 20: Recommended placement of firewalls for DirectAccess solution

The following table lists the recommended DirectAccess firewall rules for the DirectAccess solution illustrated in the previous figure. If the firewall configuration for your organization is different, then adjust the firewall rules accordingly.

Table 13: Recommended DirectAccess Firewall Rules

Firewall	Port or Protocol	Direction
Outer	IPv6	Inbound and outbound
Outer	Encapsulating Security Payload (ESP) on (IP protocol 50)	Inbound and outbound
Outer	Teredo (UDP port 3544)	Inbound
Outer	ISATAP (IP protocol 41)	Inbound and outbound
Outer	Secure HTTP (TCP port 443)	Inbound
Inner	Internet Key Exchange (UDP port 500)	Inbound and outbound
Inner	ESP (IP protocol 50)	Inbound and outbound

DirectAccess Simultaneous Internet and Intranet Access

By default, remote DirectAccess Clients are able to simultaneously access the Internet, your organization's intranet, and the local IP subnet. DirectAccess Clients are configured to send all DNS name resolution requests for intranet-based resources to DNS servers in the intranet. DirectAccess Clients send all other DNS name resolution requests to the ISP's DNS server(s). This feature is known as *split tunneling*.

You can disable split tunneling through by using Group Policy at Computer Configuration \ Administrative Templates \ Network \ Network connections \ Default value: disabled. You can also use Group Policy to configure Windows Firewall for advanced configuration options such as per-application control of split tunneling. This allows you to configure which applications are allowed to access the intranet-based resources while accessing the intranet remotely.

When split tunneling is disabled, all traffic from the DirectAccess Client will be routed to the enterprise network over an IP-HTTPS tunnel. DirectAccess Clients who have had split tunneling disabled are able to access any resources on their local link (such as network printers) but any network traffic that must cross a network router will be forwarded to the DirectAccess Server.

The IP-HTTPS protocol is always used when split tunneling has been disabled. To reduce load on the DirectAccess Server, packets which are destined for your intranet are encrypted, while packets that are destined outside your intranet are unencrypted.

DirectAccess Optional Security Components

As an additional level of security protection, you may want to deploy:

- **NAP IPsec enforcement**. This prevents unhealthy computers from being able to establish an IPsec connection. NAP IPsec enforcement provides the strongest and most flexible method for maintaining client computer compliance with network health requirements. For more information on NAP IPsec enforcement, see "Understanding NAP IPsec Enforcement" at http://technet.microsoft.com/en-us/library/cc726008.aspx.
- **Server and domain isolation**. Isolates your domain and server resources by limiting access to authenticated and authorized computers. For example, you can create a logical network consisting of computers that share a common Windows-based security framework and a set of requirements for secure communication. Each computer on the logically isolated network can provide authentication credentials to the other computers on the isolated network to prove membership. Requests for communication that originate from computers that are not part of the isolated network are ignored. For more information on server and domain isolation, see "Server and Domain Isolation" at http://technet.microsoft.com/en-us/network/bb545651.aspx.
- **Smartcard enforcement**. You can user smartcard authentication to provide the following enforcement:
    - **User enforcement**. Always require smartcard authentication, regardless of which computer the user logs on to or if the user is connecting locally or remotely, always require Smartcard for login. This feature is enabled by configuring the **Smart card required for interactive logon** option for each user.
    - **Machine enforcement**. Always require smartcard authentication, regardless who logs onto the computer or if the computer is connecting locally or remotely. This feature is enabled by configuring the Machine Settings | Local Policies | Security Options |Interactive Logon: Require Smart Card Group Policy.
    - **Gateway enforcement**. The IPsec gateway requires smartcard authentication before allowing connectivity. This option may be combined with user or machine enforcement to provide a second layer of checking that the user has logged on with a smart card. Alternatively, this option can be used without option user or machine enforcement, which means that users are be able to log onto their computer and access the Internet without a smartcard (assuming split tunneling is not disabled) but would need to insert a smart card to access any intranet-based resources.

DirectAccess Deployment Scenarios

You can deploy DirectAccess solutions to support any number of simultaneous DirectAccess clients. In addition, you can deploy DirectAccess solutions that provide higher-availability and fault tolerance to help avoid any outages. You can improve the scaling and fault tolerance of your DirectAcess clients by using one of the following deployment scenario:

- Single server
- Multiple servers with multiple roles
- Multiple servers with identical roles

Use these deployment scenarios as templates for creating your own DirectAccess solution. These deployment scenarios represent best practice recommendations that can be applied to your organization.

Single Server

In the Single Server deployment scenario, as illustrated in the following figure, all DirectAccess server-side components are running on one computer.

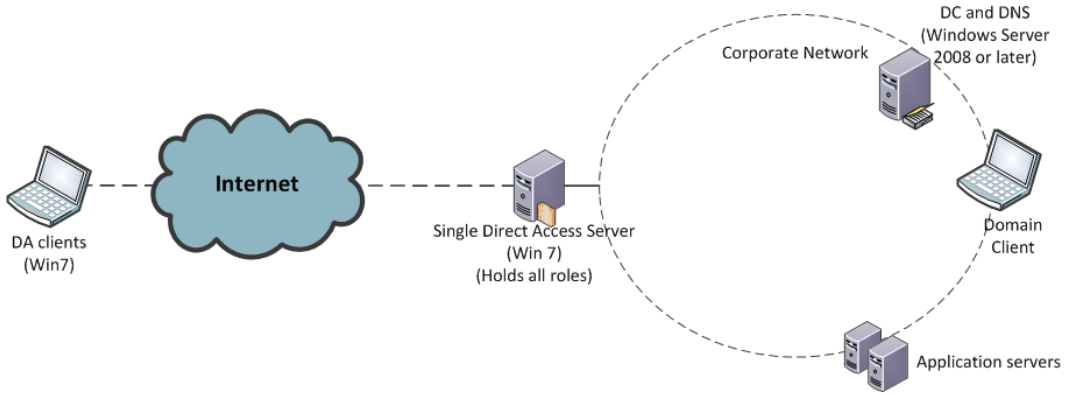

Figure 21: Single Server deployment scenario

The following table lists the benefits and limitations of the Single Server deployment scenario.

Table 14: Benefits and Limitations of the Single Server Deployment Scenario

Benefits	Limitations
Relatively simple deployment scenario, which requires a single computer running	Susceptible to a single point of failure.

DirectAccess Server.	
	Server performance bottlenecks can limit the maximum number of concurrent connections.

Multiple Servers with Multiple Roles

In the Multiple Servers with Multiple Roles deployment scenario, as illustrated in the following figure, the DirectAccess server-side components are running on more than one computer. This scenario provides improvements in scaling, but does not provide additional fault tolerance or help prevent single point of failure for DirectAccess server-side components.

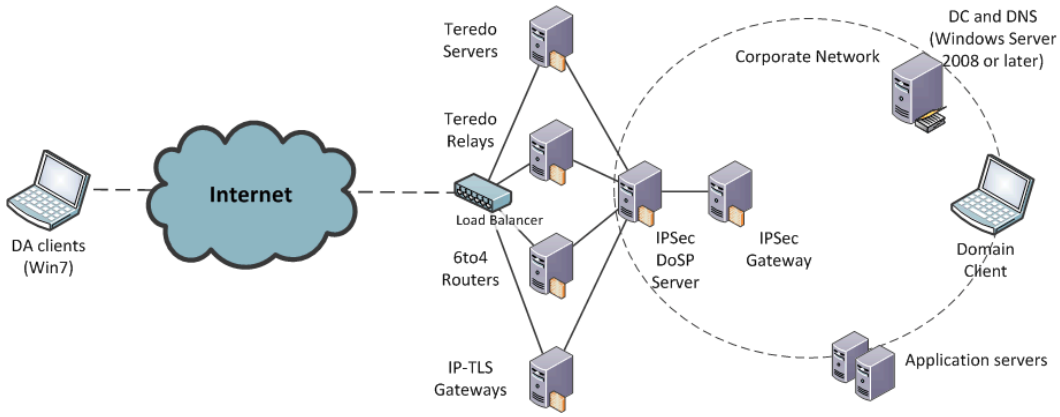

Figure 22: Multiple Servers with Multiple Roles deployment scenario

The following table lists the benefits and limitations of the Multiple Servers with Multiple Roles deployment scenario.

Table 15: Benefits and Limitations of the Multiple Servers with Multiple Roles Deployment Scenario

Benefits	Limitations
Improves scalability to support larger number of concurrent connections.	Susceptible to a single point of failure for each component.

	Requires additional hardware.
	Requires routing reconfiguration.

Multiple Servers with Identical Roles

In the Multiple Servers with Identical Roles deployment scenario, as illustrated in the following figure, all DirectAccess server-side components are running on multiple computers. This scenario provides improvements in scaling and fault tolerance. Unlike the other deployment scenarios, this scenario helps eliminate single point of failure for DirectAccess server-side components.

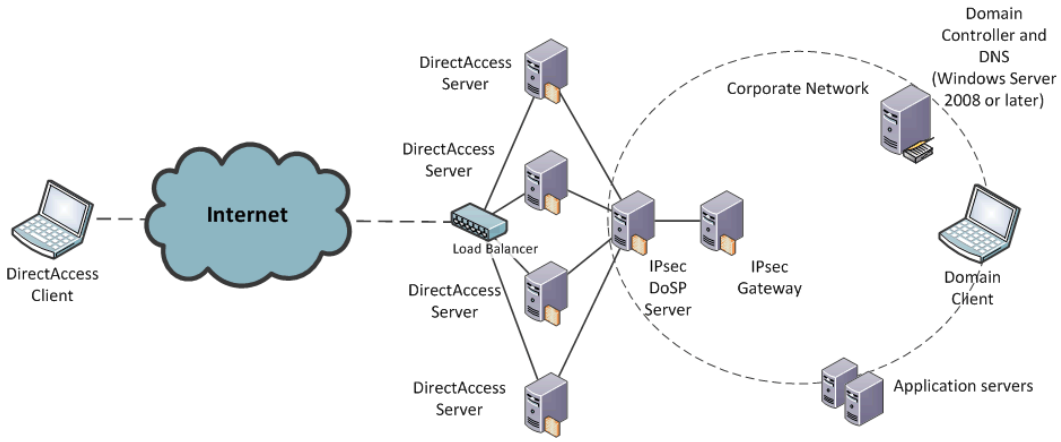

Figure 23: Multiple Servers with Identical Roles deployment scenario

The following table lists the benefits and limitations of the Multiple Servers with Identical Roles deployment scenario.

Table 16: Benefits and Limitations of the Multiple Servers with Identical Roles Deployment Scenario

Benefits	Limitations
Improves scalability to support larger number of concurrent connections.	Requires additional hardware.
Improves fault-tolerances to help eliminate single point of failure.	Requires routing reconfiguration.

DirectAccess and Failover Clustering

You can use Failover Clustering in Windows Server 2008 to improve the availability of DirectAccess Servers. You can use Failover Clustering in conjunction with or in place of the inherent fault tolerance in DirectAccess, such as provided by the Multiple Servers with Identical Roles deployment scenario.

The following DirectAccess Server components can be run as workloads in a Failover Cluster:

- 6to4 Servers
- IPsec DoSP Server
- IPsec Gateway

For more information on creating a failover cluster, see
http://www.microsoft.com/windowsserver2008/en/us/clustering-resources.aspx

Sequence for Establishing a DirectAccess Connection

The followings steps describe the sequence for establishing a DirectAccess connection between a DirectAccess client running Windows 7, the DirectAccess server, and resources on an intranet:

1. Deploy Windows 7 and DirectAccess Client connectivity policies.
2. Determine connectivity requirements between DirectAccess Client and application and resources in the intranet.
3. Establish the required connections to the DirectAccess Servers.
4. Validate the connection between the DirectAccess Client and the DirectAccess Servers.
5. Forward traffic to intranet resources.

Step 1: Deploy Windows 7 and DirectAccess Client Policy

Windows 7 needs to be deployed on the mobile computer. In addition, the DirectAccess Client policies need to be deployed. The DirectAccess Client policies can be deployed as a part of the Windows 7 image or in a subsequent deployment. The policies allow you to allow grant access to specific applications or resources to specific user while preventing access to other users. The policies control:

- The connectivity for an application, resource, or namespace thorough DirectAccess Servers.
- A schedule that limits the periods of time when remote connectivity is allowed or denied in the policy.

In addition, the DirectAccess Client needs to do name resolution for the DirectAccess Servers specified in the policy and the resources within your intranet, typically performed by DNS.

Step 2: Determine Connectivity Requirements Between Client and Intranet

The DirectAccess Client can transparently initiate the network connection between the client and the resources and applications in your organizations intranet. If an application references a computer name within the intranet, the DirectAccess client determines if the server computer must be accessed with, or without, a tunneled connection. After the DirectAccess Client determines the type of connection required, the client establishes the connection directly, through a tunnel, or both as required to access the resource.

Step 3: Establish Required Connections

The DirectAccess client connects to the DirectAccess Servers based on policy and the current connectivity available. The connection to the DirectAccess Servers is used to connect to your intranet services and resources, including DNS services, Active Directory services, and application-related resources.

Step 4: Validate Connection

The DirectAccess Server validates all incoming connections by using IPsec authentication in the "Seamless VPN" deployment scenario. After the connection is validated, the appropriate IP addresses are assigned to the DirectAccess Client. The DirectAccess Server is configured to filter out all traffic except Internet Key Exchange (IKE) and Encapsulating Security Payload (ESP) packets.

Step 5: Forward Traffic to Intranet

After the DirectAccess Client connection is validated, the DirectAccess Server creates a connection between the DirectAccess Client and resources on the intranet. If the address of the resource is published as an address provided by IPv6 Transition services, then IPv6 Transition is required.

If your organization has deployed a dual-stack IPv6, then no IPv6 to IPv4 translation is required. Otherwise, traffic between the DirectAccess Client and your intranet resources need to be translated by ISATAP or 6to4. 6to4 allows IPv6 packets to be transmitted over an IPv4 network without the need to configure explicit tunnels. 6to4 does not facilitate interoperation between IPv4-only hosts and IPv6-only hosts, but tunnels IPv6 packets through an IPv4 network, such as the Internet.

Secured Remote Connectivity for Private and Public Computers

Another common problem for remote users is the ability to access intranet-based resources from computers that are not owned by their organization, such as public computers or Internet kiosks. Without a mobile computer provided by their organization, most users are unable to access intranet-based resources.

A combination of the Remote Workspace, presentation virtualization, and Remote Desktop Services Gateway features allows users on Windows 7 clients to remotely access the intranet-based resources without requiring any additional software to be installed on the Windows 7 client. This allows the users to remotely access their desktop as though they were working from their computer on the intranet, as illustrated in the following figure.

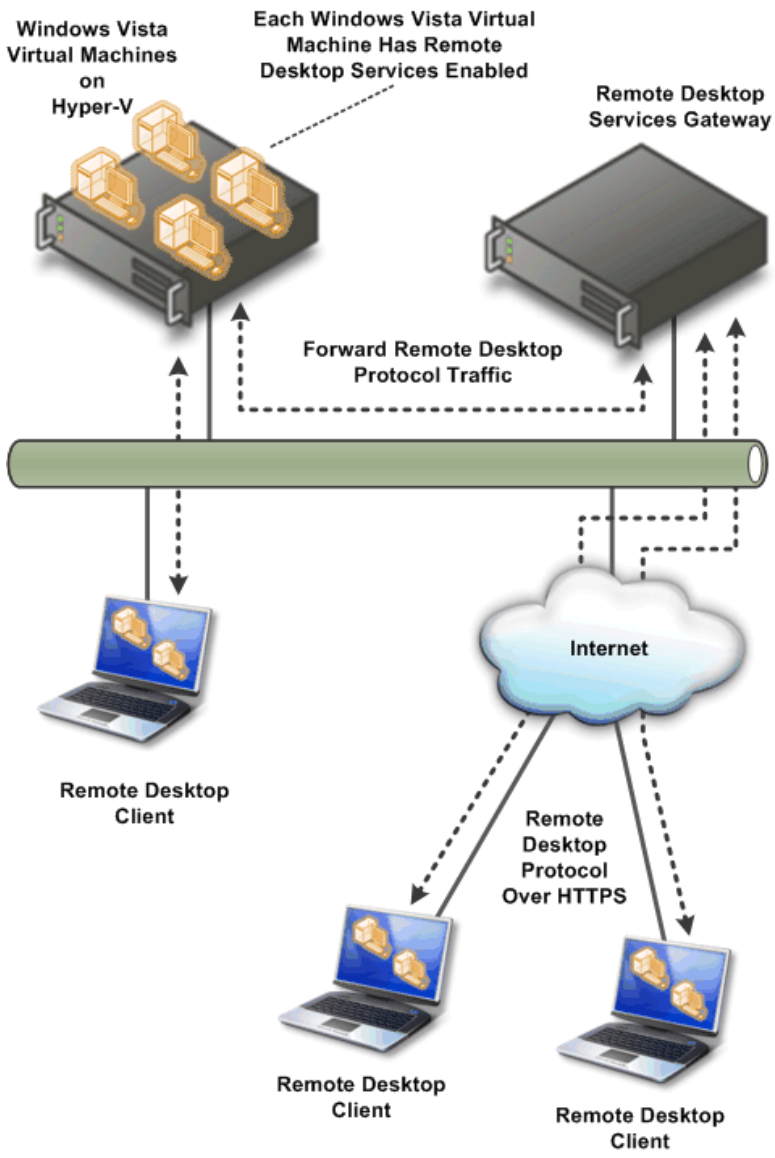

Figure 24: Remote user connected to an intranet by using Remote Workspace, presentation virtualization, and Remote Desktop Services Gateway

From the user's perspective, the desktop on the remote Windows 7 client transforms the look of the user's desktop on the intranet, including icons, Start menu items, and installed applications are identical to the user experience on their computer on the intranet. When the remote user closes the remote session, the remote Windows 7 client desktop environment reverts to the previous configuration.

Improved Performance for Branch Offices

One of the largest problems facing branch offices is how to improve the performance of accessing intranet resources in other locations, such as the headquarters or regional data centers. Typically branch offices are connected by wide area networks (WANs) which usually have slower data rates than your intranet. Reducing the network utilization on the WAN network segments provides available network bandwidth for applications and services.

The BranchCache feature in Windows Server 2008 R2 and Windows 7 reduces the network utilization on WAN segments that connect branch offices by locally caching frequently used files on computers in the branch office. The type of content that is cached is content returned by Server Message Block (SMB) requests and HTTP requests.

The following figure contrasts branch office network utilization with and without the BranchCache feature.

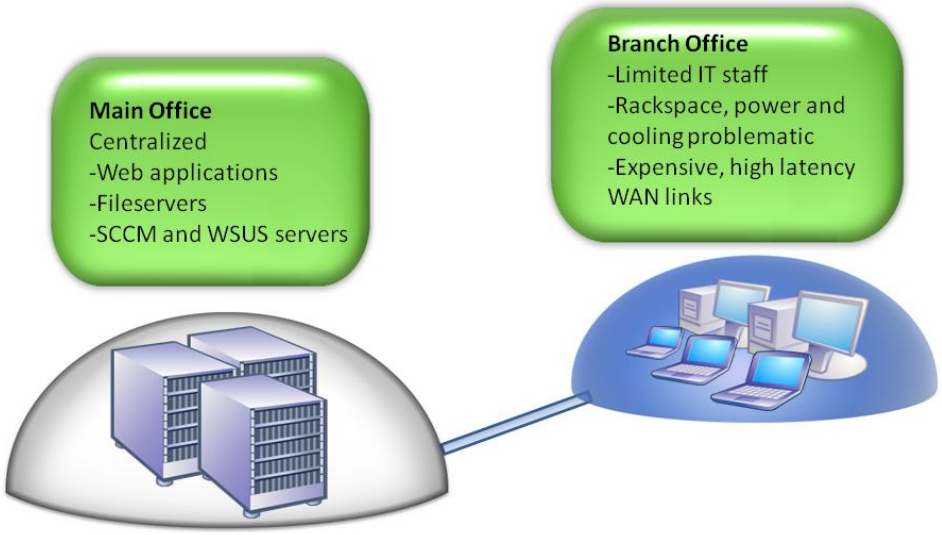

Figure 25: The branch office problem

BranchCache Modes

BranchCache supports the following operational modes:

- Distributed Mode
- Hosted caching

Distributed Mode

In distributed mode, content is cached on the branch on client computers running Windows 7. The disadvantage to this solution is that content is cached on client computers, so if the computer containing the cached content is unavailable, the content must be retrieved over the WAN connection, as illustrated in the following figure.

The following sequence reflects how the distributed mode caches content:

1. A client computer downloads content from a BranchCache enabled server in the main office. It adds this content to a cache stored on its hard disk.
2. A second client computer accesses the same content. The server returns identifiers that describe the piece of desired content. The computer searches the local network for other computers that have already downloaded the content.
3. The second computer discovers the piece of content in the cache of the first computer. The second computer downloads the content from the first machine.

If a client computer cannot locate a piece of content on the local network, it will return to the server and request a full download.

Hosted Caching Mode

In the hosted caching mode, content is cached on the branch on client computers running Windows Server 2008 R2. The advantage to this mode is that the server is always available, so the cached content is always available. The unavailability of any client computer running Windows 7 does not affect the availability of the content cache, as illustrated in the following figure.

The following sequence reflects how the hosted caching mode caches content:

1. A client computer downloads content from a BranchCache enabled server in the main office. It adds this content to a cache stored on its hard disk.
2. A second client computer accesses the same content. The server returns identifiers that describe the piece of desired content. The computer searches the local network for other computers that have already downloaded the content.
3. The second computer discovers the piece of content in the cache of the first computer. The second client downloads the content from the first computer.

If a client computer cannot locate a piece of content on the local network, the client computer will return to the server and request a full download

BranchCache Management

BranchCache behavior can be configured by using Group Policy. Windows Server 2008 R2 includes a Group Policy administrative template that can be used to administer the BranchCache configuration settings.

You can also manage BranchCache by using the NetSH command. For more information configuring BranchCache by using the NetSH command, see "NetSH Command Index" in *Windows Branch Cache Deployment Guide*.

Improved Security for Branch Offices

Windows Server 2008 RTM introduced the Read-only Domain Controller feature, which allows a read-only copy of AD DS to be placed in less secured environments, like branch offices. Windows Server 2008 R2 introduces support for read-only copies of information stored in Distributed File System (DFS), as illustrated in the following figure.

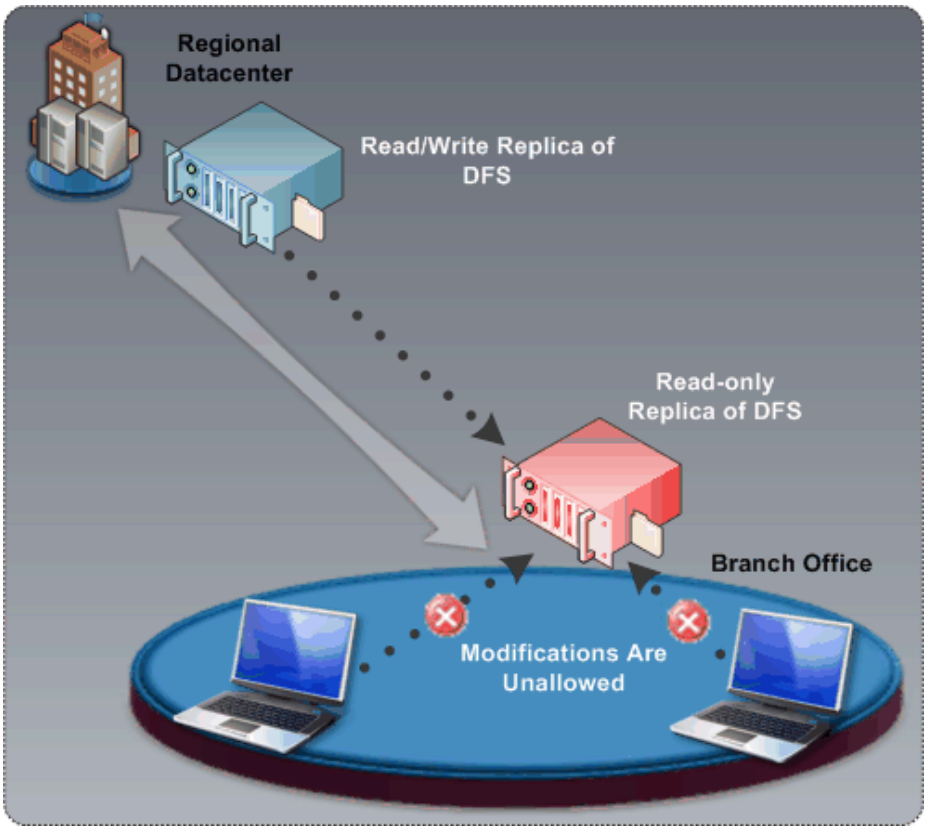

Figure 26: Read-only DFS in a branch office scenario

Read-only DFS helps protect your digital assets by allowing branch offices read-only access to information that you replicate to them by using DFS. Because the information is read-only, users are unable to modify the content stored in read-only DFS replicated content and no content changes are replicated to other DFS replica copies in other locations.

Improved Efficiency for Power Management

Windows 7 includes a number of power management features that allow you to control power utilization in your organization with a finer degree of granularity than in previous operating systems. Windows 7 allows you to take advantages of the latest hardware developments for reducing power consumption in desktop and laptop computers.

Windows Server 2008 R2 includes a number of Group Policy settings that allow you to centrally manage the power consumption of computers running Windows 7.

Virtualized Desktop Integration

Windows 7 introduces the desktop and applications feed feature, which helps integrate desktops and applications virtualized by using Remote Desktop Services with the Windows 7 user interface. This integration makes the user experience for running virtualized applications or desktops the same as running the applications locally.

Windows 7 can be configured to subscribe to desktop and application feeds provided by Remote Desktops and RemoteApp programs. These feeds are presented to Windows 7 users using the new RemoteApp and Desktop Connection control panel applet. The RemoteApp and Desktop Web Access control panel applet provides the ability to connect to resources from Windows Vista and Windows XP in addition to Windows 7.

The desktop and applications feeds feature includes the following capabilities:

- Users can subscribe to RemoteApp programs and Remote Desktops by using the RemoteApp and Desktop Connections control panel applet.
- User experience is seamlessly integrated with Windows 7 because:
    - The RemoteApp programs desktops are added to the Start Menu.
    - A new System Tray icon shows connectivity status to all of the connections to feeds.
- The administration for RemoteApp, Remote Desktop, and RemoteApp and Desktop Web Access is performed through a unified infrastructure.
- RemoteApp and Desktop Web Access provide access to RemoteApp and Remote Desktops to previous Windows operating systems by using a Web-based interface.

- Provides supports for managed computers (member computers in an Active Directory domain) and unmanaged computers (standalone computers).
- User interface always reflects applications and desktops in the Start Menu and in the web-based interface as they are added by the administrator.
- Access to all desktops and applications requires a single sign-on.

Higher Fault Tolerance for Connectivity Between Sites and Locations

One of the most common scenarios facing organizations today is connectivity between sites and locations. Many organizations connect their sites and locations by using VPN tunnels over public networks, such as the Internet.

One of the problems with existing VPN solutions is they are not resilient to connection failures or device outages. When any outage occurs, the VPN tunnel is terminated and the VPN tunnel must be re-established, resulting in momentary outages in connectivity.

The Agile VPN feature in Windows Server 2008 R2 allows a VPN to have multiple network paths between points in the VPN tunnel. In the event of a failure, Agile VPN automatically uses another network path to maintain the existing VPN tunnel, without interruption of connectivity.

Protection for Removable Drives

In Windows Server 2008 and prior operating systems, BitLocker Drive Encryption (BitLocker) was primarily used to protect the operating system volume. Information stored on other volumes, including removable media, was encrypted by using Encrypted File System (EFS).

In Windows 7, you can use BitLocker to encrypt removable drives, such as eSATA hard disks, USB hard disks, USB thumb drivers, or compact flash drives. This allows you to protect information stored on removable media with the same level of protection as the operating system volume.

BitLocker requires the use of a Trusted Platform Module (TPM) device or physical key to access information encrypted by BitLocker. You can also require a personal identification number (PIN) in addition to the TPM device or physical key.

The keys for BitLocker can also be archived in AD DS, which provide an extra level of protection in the event the physical key is lost or the TPM device fails. This integration between Windows 7 and Windows Server 2008 R2 allows you to protect sensitive information without worrying about users losing their physical key.

Prevention of Data Loss for Mobile Users

The Offline Files feature allows you to designate files and folders stored on network shared folders for use even when the network shared folders are unavailable (offline). For example, a mobile user disconnects a laptop computer from your intranet and works from a remote location.

The Offline Files feature has the following operation modes:

- **Online mode**. The user is working in online mode when they are connected to the server and most file requests are sent to the server.
- **Offline mode**. The user is working in offline mode when they are not connected to the server and all file requests are satisfied from the Offline Files cache stored locally on the computer.

In Windows Server 2008 RTM and Windows Vista, the Offline Files feature was configured for online mode by default. In Windows Server 2008 R2 and Windows 7, the Offline Files feature supports transitioning to offline mode *when on a slow network* by default. This helps reduce the network traffic while connected to your intranet because the users are modifying locally cached copies of the information stored in the Offline Files local cache. However, the information stored in the Offline Files local cache is still protected from loss because the information is synchronized with the network shared folder.

Summary

Microsoft Windows Server® 2008 R2 gives IT Professionals more control over their server and network infrastructure, and provides an enterprise-class foundation for business workloads. Microsoft enables organizations to deliver rich Web-based experiences efficiently and effectively, by reducing the amount of effort required to administer and support your Web-based applications. The powerful Virtualization technologies in Windows Server 2008 R2 enable you to increase your server consolidation ratios, while reducing the amount of administrative effort required for managing the infrastructure. Through increased automation and improved remote administration, Windows Server 2008 R2 helps organizations save money and time, by reducing travel expenses, decreasing energy consumption, and automating repetitive IT tasks. When combined with Windows 7 client operating system, the Virtual Desktop Infrastructure in Windows Server 2008 enables you to provide your employees with anywhere access to corporate data and resources, while helping to maintain the security of your enterprise systems.