

Windows Server 2008 R2 Reviewers Guide

Published: July 2009

© 2009 Microsoft Corporation. All rights reserved. This document is developed prior to the product’s release to manufacturing, and as such, we cannot guarantee that all details included herein will be exactly as what is found in the shipping product. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. The information represents the product at the time this document was printed and should be used for planning purposes only. Information subject to change at any time without prior notice. This whitepaper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Microsoft, Active Directory, Aero, BitLocker, Forefront, Excel, Hyper-V, SQL Server, Visual Studio, Windows, Windows Media, Windows PowerShell, the Windows logo, Windows Vista, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Summary

The Windows Server® 2008 R2 Reviewers Guide provides a technical overview of the incremental features and functions that make Windows Server 2008 R2 the next-generation Windows Server operating system and successor to Windows Server 2008. This guide also provides information about the benefits Windows Server 2008 R2 offers diverse users, as well as information about different scenarios.

Table of Contents

[Introduction to Windows Server® 2008 R2 1](#_Toc235952514)

[Overview 1](#_Toc235952515)

[Using this Guide 1](#_Toc235952516)

[Getting Started 3](#_Toc235952517)

[System Requirements 3](#_Toc235952518)

[Installation and Activation 4](#_Toc235952519)

[Windows Server 2008 R2 Installation 4](#_Toc235952520)

[Virtualization 7](#_Toc235952521)

[Improved Virtualization with Hyper-V 8](#_Toc235952522)

[Increased Availability for Virtual Data Centers 8](#_Toc235952523)

[Live Migration Support through Cluster Shared Volumes 8](#_Toc235952524)

[Improved Cluster Node Connectivity Fault Tolerance 10](#_Toc235952525)

[Enhanced Cluster Validation Tool 14](#_Toc235952526)

[Improved Migration of Cluster Workloads 15](#_Toc235952527)

[Improved Management of Virtual Data Centers 20](#_Toc235952528)

[Simplified Method for Physical and Virtual Computer Deployments 20](#_Toc235952529)

[Processor Compatibility for Live Migration 21](#_Toc235952530)

[Increased Performance and Hardware Support for Hyper-V Virtual Machines 21](#_Toc235952531)

[Improved Virtual Networking Performance 22](#_Toc235952532)

[Terminal Services Becomes Remote Desktop Services for Improved Presentation Virtualization 22](#_Toc235952533)

[Remote Desktop Services and Virtual Desktop Infrastructure 23](#_Toc235952534)

[Management 30](#_Toc235952535)

[Improved Data Center Power Consumption Management 30](#_Toc235952536)

[Improve the Power Efficiency of Individual Servers 31](#_Toc235952537)

[Processor Power Management 32](#_Toc235952538)

[Storage Power Management 32](#_Toc235952539)

[Additional Power Saving Features 33](#_Toc235952540)

[Measure and Manage Power Usage Across the Organization 34](#_Toc235952541)

[Remote Manageability of Power Policy 34](#_Toc235952542)

[In-Band Power Metering and Budgeting 35](#_Toc235952543)

[New Additional Qualifier for the Designed for Windows Server 2008 R2 Logo Program 35](#_Toc235952544)

[Improved Remote Administration 36](#_Toc235952545)

[Reduced Administrative Effort for Interactive Administrative Tasks 36](#_Toc235952546)

[Enhanced Command-line and Automated Management 37](#_Toc235952547)

[Improved Identity Management 40](#_Toc235952548)

[Improvements for All Active Directory Server Roles 41](#_Toc235952549)

[Improvements in Active Directory Domain Services (AD DS) 43](#_Toc235952550)

[Improvements in Active Directory Federated Services 52](#_Toc235952551)

[Improved Compliance with Established Standards and Best Practices 53](#_Toc235952552)

[Web 54](#_Toc235952553)

[Reduced Effort to Administer and Support Web-based Applications 54](#_Toc235952554)

[Reduced Support and Troubleshooting Effort 58](#_Toc235952555)

[Improved FTP Services 59](#_Toc235952556)

[Ability to Extend Functionality and Features 60](#_Toc235952557)

[Improved .NET Support 61](#_Toc235952558)

[Improved Application Pool Security 61](#_Toc235952559)

[IIS.NET Community Portal 61](#_Toc235952560)

[Solid Foundation for Enterprise Workloads 62](#_Toc235952561)

[Scalability and Reliability 62](#_Toc235952562)

[Leveraging Sophisticated CPU Architectures 62](#_Toc235952563)

[Increased Operating System Componentization 62](#_Toc235952564)

[Improved Performance and Scalability for Applications and Services 63](#_Toc235952565)

[Improved Storage Solutions 66](#_Toc235952566)

[Improved Protection of Intranet Resources 68](#_Toc235952567)

[Improved Management of File Services 69](#_Toc235952568)

[Improvements in Backup and Recovery 72](#_Toc235952569)

[Better Together with Windows 7 77](#_Toc235952570)

[Simplified Remote Connectivity for Corporate Computers 77](#_Toc235952571)

[Secured Remote Connectivity for Private and Public Computers 82](#_Toc235952572)

[Improved Performance for Branch Offices 82](#_Toc235952573)

[Improved Security for Branch Offices 91](#_Toc235952574)

[More Efficient Power Management 92](#_Toc235952575)

[Improved Virtualized Desktop Integration 92](#_Toc235952576)

[Higher Fault Tolerance for Connectivity Between Sites 93](#_Toc235952577)

[Increased Protection for Removable Drives 93](#_Toc235952578)

[Improved Prevention of Data Loss for Mobile Users 93](#_Toc235952579)

# Introduction to Windows Server® 2008 R2

Windows Server 2008 R2, built with Web and virtualization technologies, is the most robust, secure, and reliable foundation on which to develop, deliver, and manage rich user experiences and applications.

## Overview

Windows Server 2008 R2 builds on the award-winning foundation of Windows Server 2008, expanding existing technology and adding new features to enable IT professionals to increase the reliability and flexibility of their server infrastructures. New virtualization tools, Web resources, management enhancements, and exciting Windows™ 7 integration help save time, reduce costs, and provide a platform for a dynamic and efficiently managed data center. Powerful tools such as Internet Information Services (IIS) version 7.0, updated Server Manager and Hyper-V™ platforms and Windows PowerShell™ version 2.0 combine to give customers greater control, increased efficiency and the ability to react to front-line business needs faster than ever before.

## 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 following figure outlines the technology investments areas of Windows Server 2008 R2:

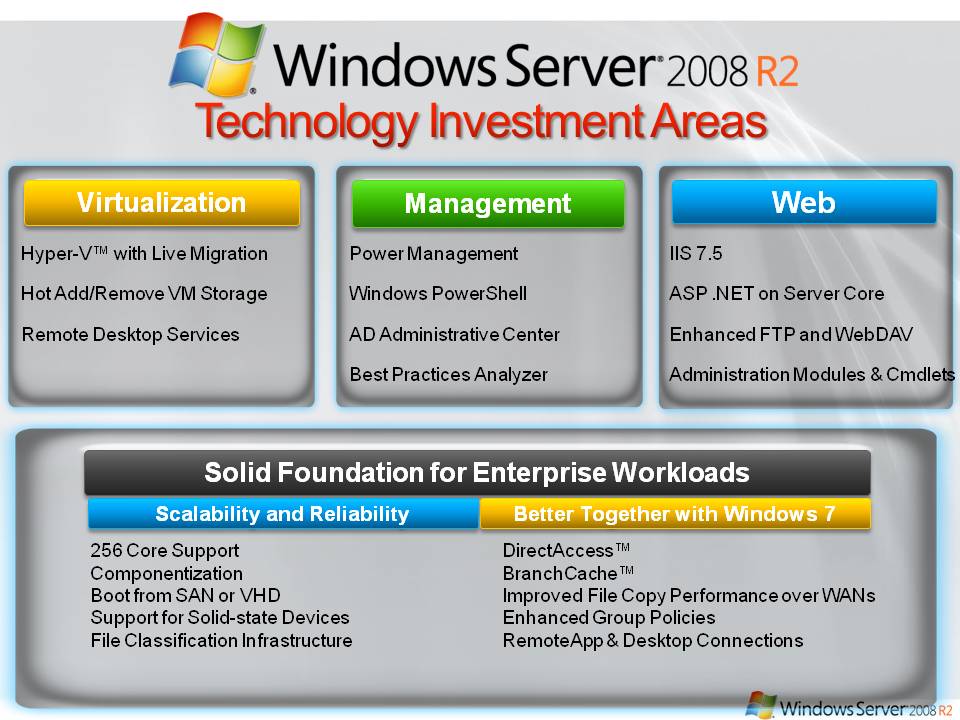


Figure 1: Windows Server 2008 R2 technology investments

The key technology investments in Windows Server 2008 R2 include:

* **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**. With enterprise IT departments shouldering ever-heavier burdens, Windows Server 2008 R2 has been designed specifically with heavier workloads for both across server and client computing. On the server side, R2 includes architectural enhancements for more compute power and role componentization as well as specific features 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.

# Getting Started

To evaluate Windows Server® 2008 R2, you need to install Windows Server 2008 R2 in your test or evaluation environment. After you install Windows Server 2008 R2, you can use this guide to help you explore the key technology investments for yourself.

## System Requirements

Before you install Windows Server 2008 R2, you need to ensure that the physical or virtual computer being used in your evaluation has the appropriate system resources. The following table lists the system requirements for Windows Server 2008 R2.

Table 1: Window Server 2008 R2 System Requirements

|  |  |
| --- | --- |
| **Component** | **Requirement** |
| **Processor** | • Minimum: 1.4GHz x64 processor • Recommended: 2GHz or faster |
| **Memory** | • Minimum: 512MB RAM • Recommended: 2GB RAM or greater • Maximum 32GB (Standard) or 2TB (Enterprise and Datacenter Editions) |
| **Available Disk Space** | • Minimum: 10GB • Recommended: 40GB or greater **Note:** Computers with more than 16GB of RAM will require more disk space for paging, hibernation, and dump files |
| **Drive** | DVD-ROM drive |
| **Display and Peripherals** | • Super VGA (800 x 600) or higher-resolution monitor • Keyboard • Microsoft Mouse or compatible pointing device |

The actual requirements will vary based on your system configuration and the applications and features you choose to install. Processor performance is dependent upon not only the clock frequency of the processor, but also the number of cores and the size of the processor cache. Disk space requirements for the system partition are approximate. Additional available hard-disk space may be required if you are installing over a network.

## Installation and Activation

If you plan to install this release of Windows Server 2008 R2 on your primary machine, it is recommended that you back up your existing data prior to installation.

### Windows Server 2008 R2 Installation

Prior to installation of Windows Server 2008 R2, you need to determine if you will deploy Windows Server 2008 R2 in a physical environment or a virtual environment. If you are installing Windows Server 2008 R2 in a physical environment, all you need is the Windows Server 2008 R2 distribution media.

To install this release of Windows Server 2008 R2, perform the following steps:

1. Start the physical computer with the Windows Server 2008 R2 distribution media, by inserting the distribution media into the computer’s DVD-ROM drive.

For a virtual machine, mount the .iso file image of the Windows Server 2008 R2 distribution media on the virtual machine and then start the virtual machine.

**Note:** Ensure that you configure the virtual machine to support x64 processors because Windows Server 2008 R2 is only supported on x64 processors.

1. On the **Install Windows** page of the installation process (as illustrated in the following figure), select the appropriate language, time and currency format, and keyboard, and then click **Next**.
2. On the **Select the operating system you want to select Full Installation**, and then click **Next**.

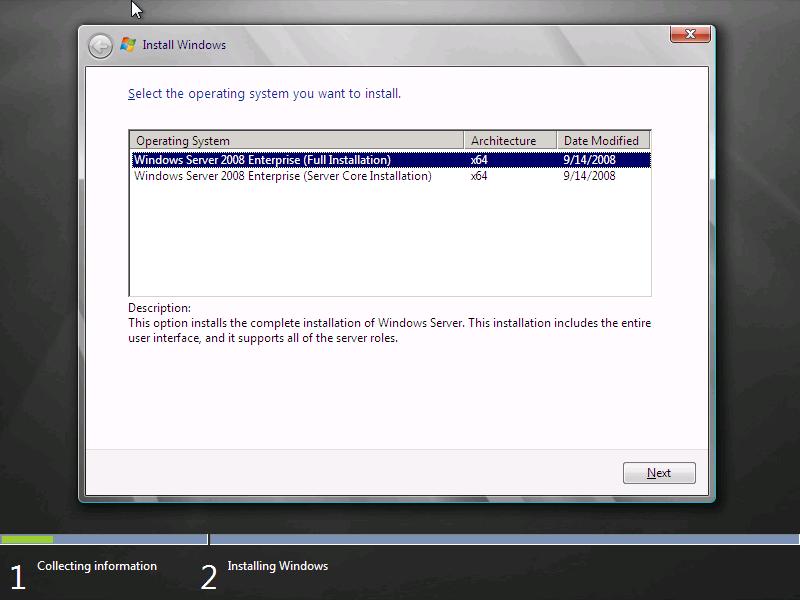


Figure 2: Windows Server 2008 R2 operating system installation options

Notice that Windows Server 2008 R2 is now available only over a 64-bit processor architecture. Although you can install Windows Server 2008 R2 by using the Full Installation or Server Core Installation option, this guide assumes that you select the Full Installation option.

**Note:** After you have completed your installation, you cannot change the installation option from the Full Installation option to the Server Core installation, or vice versa, without reinstalling Windows Server 2008 R2.

1. The Windows Server 2008 R2 installation process continues until Windows Server 2008 R2 starts for the first time.
2. After Windows Server 2008 R2 starts, log on as a user that is a member of the local Administrators group.
3. Add, partition, and format any additional disks you require for your evaluation.
4. Add any additional network adapters that you require for your evaluation.
5. Configure the IP addressing settings for all network adapters to allow the appropriate connectivity within your environment.

**Note:** Ensure that you provide statically configured IP version 4 (IPv4) and IP version 6 (IPv6) addresses as required for your evaluation. Do not use IP addresses that are dynamically assigned by Dynamic Host Configuration Protocol (DHCP).

1. Add the appropriate Windows Server 2008 R2 server roles and features by using Server Manager.
2. Configure each server role and feature as required for your evaluation.
3. Start your evaluation of Windows Server 2008 R2.

# Virtualization

Virtualization is a major part of today’s data centers. The operating efficiencies offered by virtualization allow organizations to dramatically reduce operational effort and power consumption.

Windows Server® 2008 R2 provides the following virtualization types:

* **Client and Server virtualization provided by Hyper-V™**. Hyper-V virtualizes the system resources of a physical computer. Server virtualization allows you to provide a virtualized environment for operating systems and applications. When used alone, Hyper-V is typically used for server computer virtualization. When Hyper-V is used in conjunction with Virtual Desktop Infrastructure (VDI), Hyper-V is used for client virtualization.
* **Presentation virtualization**. This type of virtualization provided by Remote Desktop Services’ RemoteApp (see below for more information on the Terminal Services’ name change in Windows Server 2008 R2) virtualizes a processing environment and isolates the processing from the graphics and I/O, making it possible to run an application in one location but have it be controlled in another. Presentation virtualization allows end users to run a single application, or a complete desktop offering multiple applications.

**Note:** There are other types of virtualization that are not discussed in this guide, such as application virtualization provided by Microsoft App-V. For more information on all Microsoft virtualization products and technologies, see the Microsoft Virtualization home page at <http://www.microsoft.com/virtualization/default.mspx>.

## Improved Virtualization with Hyper-V

Beginning with Windows Server 2008, server virtualization using Hyper-V technology has been an integral part of the operating system. Windows Server 2008 R2 introduces a new version of Hyper-V.

Hyper-V in Windows Server 2008 R2 includes three core areas of improvement for creating dynamic virtual data centers:

* Increased availability for virtualized data centers
* Improved management of virtualized data centers
* A simplified method for physical and virtual computer deployments by using .vhd files

### Increased Availability for Virtual Data Centers

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 consolidation, high availability and most of all sophisticated management tools.

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

### Live Migration Support through Cluster Shared Volumes

Live Migration uses the new Cluster Shared Volumes (CSV) feature within Failover Clustering in Windows Server 2008 R2. The CSV volumes enable multiple nodes in the same failover cluster to concurrently access the same logical unit number (LUN). From a VM’s perspective, each VM appears to actually own a LUN; however, the .vhd files for each VM are stored on the same CSV volume, as illustrated in the following figure.

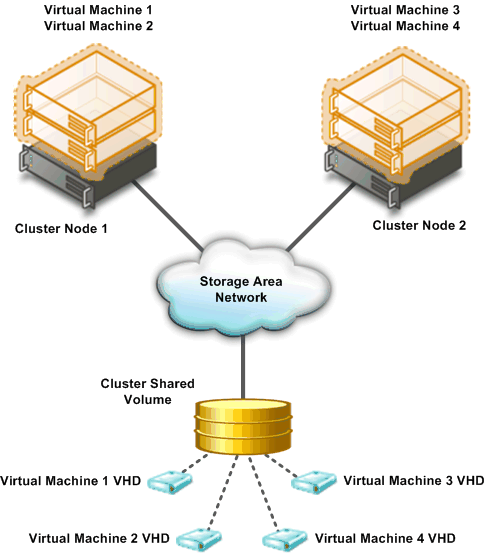


Figure 3: Cluster Shared Volumes

Because CSV provides a consistent file namespace to all nodes in the cluster, any files stored on a CSV have the same name and path from any node in the cluster. CSV volumes are stored as directories and subdirectories beneath the ClusterStorage root folder, as illustrated in the following figure.

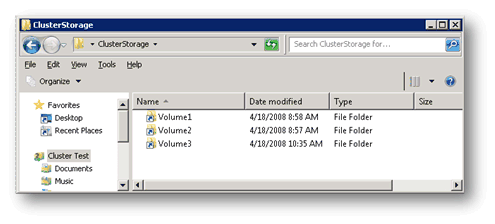


Figure 4: Example of single namespace in CSV

As illustrated in the previous figure, the CSV volumes (Volume1, Volume2, and Volume3) are stored in the ClusterStorage folder. If the ClusterStorage folder exists in the root of E:, the fully qualified path to each of the CSV volumes would be as follows:

* E:\ClusterStorage\Volume1\root
* E:\ClusterStorage\Volume2\root
* E:\ClusterStorage\Volume3\root

All cluster nodes would access the shared volumes by using these fully qualified paths.

While CSVs are currently employed mainly for Live Migration, their benefits will extend beyond that single scenario. For one, they’re easy to configure using simple NTFS rather than some other proprietary format. That means administrators won’t have to reformat their SANs to take advantage of CSVs. It also means administrators will have an easier time showing users only a single data repository rather than a small forest of silos—no more drive letter metaphors for end-users just convenient networked storage. And last, CSVs don’t require config and management tools of their own. Windows Server administrators used to the tools in Windows Server 2008 can continue using those same consoles and they’ll simply work with CSVs in R2.

### Improved Cluster Node Connectivity Fault Tolerance

Because of the architecture of CSV, there is improved cluster node connectivity fault tolerance that directly affects VMs running on the cluster. The CSV architecture implements a mechanism, known as dynamic I/O redirection, where I/O can be rerouted within the failover cluster based on connection availability, as illustrated in the following figure.

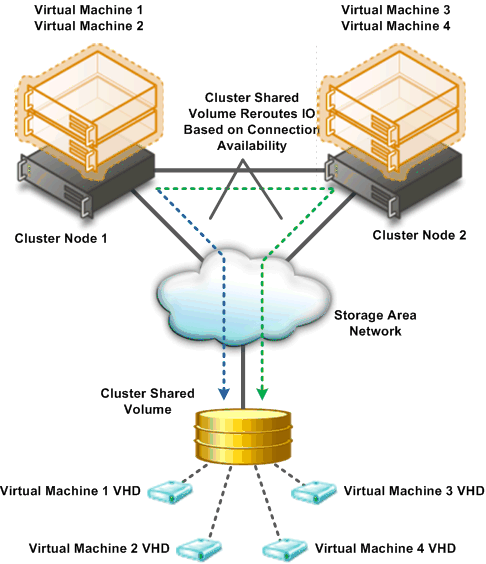


Figure 5: Dynamic IO redirection for Cluster Shared Volumes

The first type of failure that can be redirected is the failure of a cluster node connection to the shared storage between cluster nodes, typically on a Storage Area Network (SAN). As shown in the following figure, if the SAN connection on Node 2 fails, the I/O operations are redirected over the network to Node 1. Node 1 then performs the I/O operation to the SAN. This allows you do a Live Migration of the VM running on Node 2 to Node 1.

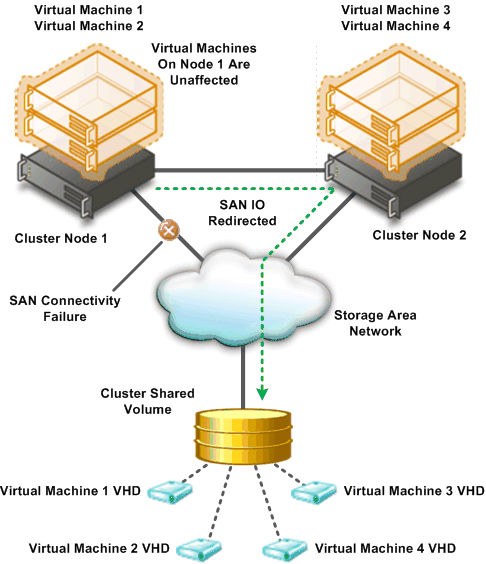


Figure 6: IO connectivity fault tolerance for CSV

The next type of failure that can be redirected is the failure of network connectivity for a cluster node. As shown in the following figure, the primary network connection between Node 1 and Node 2 fails. Node 2 automatically reroutes network traffic over a redundant network connection and Node 1 performs the network I/O.

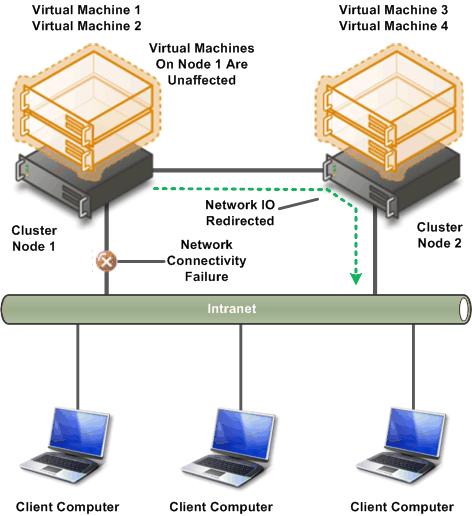


Figure 7: Network fault tolerance for CSV

The next type of failure that can be redirected is the failure of an entire cluster node. As shown in the following figure, Node 1 has ownership of a volume that is used by the VM running on Node 2. In the event of a complete failure of Node 1, ownership of the volume is changed to Node 2 without any interruption of service to the VM running on Node 2.

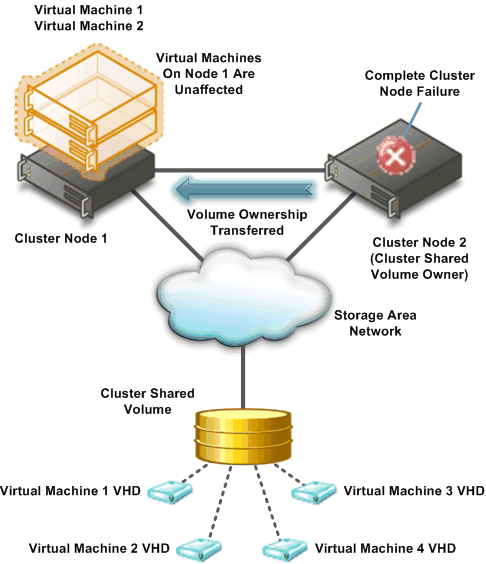


Figure 8: Node fault tolerance for CSV

### Enhanced Cluster Validation Tool

Windows Server 2008 R2 includes a Best Practices Analyzer (BPA) for all major server roles, including Failover Clustering. This analyzer examines the best practices configuration settings for a cluster and cluster nodes. The test runs only on computers that are currently cluster nodes.

### Improved Migration of Cluster Workloads

Administrators 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 DFS-N, DHCP, DTC, File Server, Generic Application, Generic Script, Generic Service, iSNS, MSMS, NFS, Other Server, TSSB, and WINS.
* Supports most common network configurations.
* Does not support rolling upgrades of clusters. (Cluster workloads must be migrated to a new cluster running Windows Server 2008 R2.)

#### Integration of Live Migration and Failover Clustering

Live Migration requires failover clustering in Windows Server 2008 R2. Specifically, Live Migration can make use of the new Cluster Shared Volumes (CSV) feature contained in Windows Server 2008 R2.

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 storage.
* The .vhd files for the virtual machines to be moved by Live Migration must be stored on the same shared storage.

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

##### Fig_01_TDM_Whitepaper_LiveMigration_Overview.gif

Figure 9: Typical configuration to support Live Migration

#### Live Migration Process

The Live Migration process is performed in the following steps:

1. An 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.

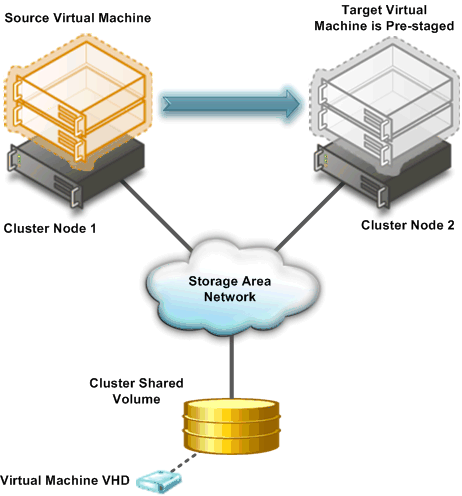


Figure 10: Creation of target virtual machine on target cluster node

1. All of the current memory in the source virtual machine is copied to the target virtual machine, as illustrated in the previous figure.
2. Clients connected to the source virtual machine continue to run on the source virtual machine and create mirrored memory pages as illustrated in the following figure.
3. The mirrored memory pages are tracked and continue an iterative copy of the dirty memory pages until all memory pages are copied to the target virtual machine, as illustrated in the following figure.

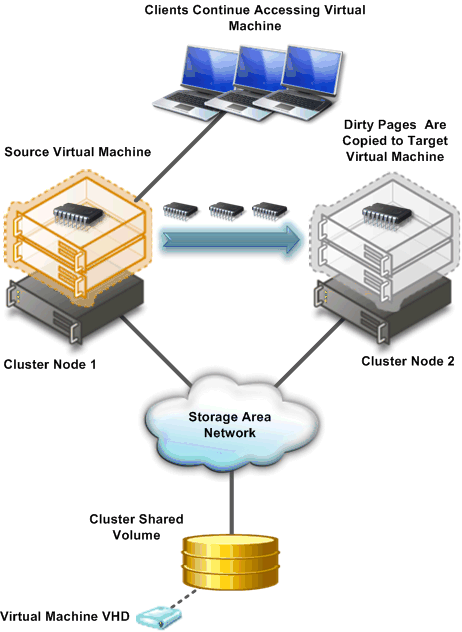


Figure 11: Iterative copy of mirrored memory from source to target virtual machine

1. When all memory pages are copied to the target virtual machine, clients are automatically redirected to the target virtual machine and the source virtual machine is deleted, as illustrated in the following figure.

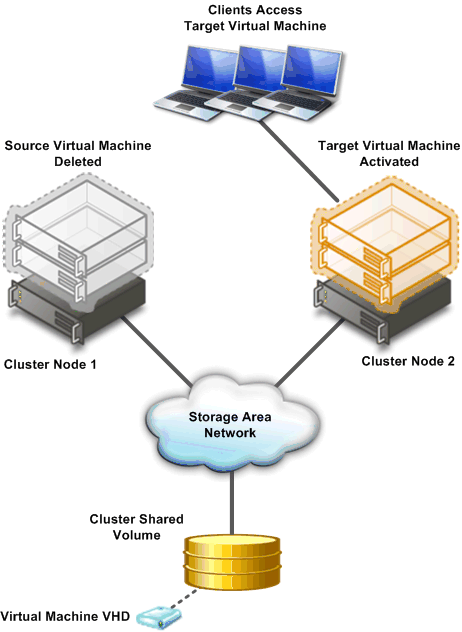


Figure 12: Final configuration after Live Migration completes

### Improved Management of Virtual Data Centers

Even with all the efficiency gained from 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. Therefore, 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 the Hyper-V Management Console**. The Hyper-V Management Console has been updated to reduce the amount of effort required to perform common day-to-day administrative tasks.
* **Enhanced command-line interface and automated management of Hyper-V administrative tasks by using Windows PowerShell™ cmdlets**.
* **Improved management of multiple Hyper-V servers in a virtual data center environment by using System Center Virtual Machine Manager 2008**. For more information on System Center Virtual Machine Manager 2008, see “Microsoft System Center Virtual Machine Manager” at <http://www.microsoft.com/systemcenter/virtualmachinemanager/en/us/default.aspx>.

### Simplified Method for Physical and Virtual Computer Deployments

Historically, different methods have been used to deploy operating systems and applications to physical and virtual computers. For virtual computers, the .vhd file format has become a *de facto* standard for deploying and interchanging preconfigured operating systems and applications. Hyper-V in Windows Server 2008 R2 supports two important updates concerning .vhd files.

First, administrators can now add and remove vhd files, as well as pass-through disks attached to a virtual SCSI controller on a running VM, without requiring a reboot. This offers more flexibility when it comes to handling storage growth needs without requiring additional downtime. It also provides more flexibility in data center backup scenarios as well as new scenarios in complex Microsoft® Exchange and SQL Server® deployments.

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 preconfigured .vhd files for deploying virtual and physical computers. This helps reduce the number of images you need to manage and provides an easier method for test deployment prior to deployment in your production environment.

### Processor Compatibility for Live Migration

Windows Server 2008 R2 Hyper-V also introduces a new feature named Processor Compatibility Mode for live migration. This feature was implemented to expand customers’ options when it comes to live migrating VMs across different CPU versions from the same processor manufacture (e.g. Intel-to-Intel and AMD-to-AMD). Previously, any Live or Quick Migration operation had to be conducted across hosts with identical CPUs.

Processor compatibility is disabled by default, but can be activated either via the Hyper-V Manager or System Center Virtual machine Manager 2008 R2. It is most applicable to Hyper-V’s Live Migration (new with R2), but Quick Migration or standard Save/Restore operations can also benefit from it. Lastly, processor compatibility is supported by any Hyper-V-enabled CPU which supports hardware assisted virtualization; however, it is important to note that it supports migration only across CPUs versions in the same product family (i.e., Intel-to-Intel or AMD-to-AMD). Cross-vendor CPU migration is not supported mainly due to differing instruction sets implemented by different CPU vendors.

### Increased Performance and Hardware Support for Hyper-V Virtual Machines

Hyper-V in Windows Server 2008 R2 now supports up to 64 logical processors in the host processor pool. This is a significant upgrade from previous versions and allows not only greater VM density per host, but also gives IT administrators more flexibility in assigning CPU resources to VMs. The new Hyper-V also adds performance enhancements that increase virtual machine performance and power consumption. First, Hyper-V now supports Second Level Address Translation (SLAT), which uses new features on today’s CPUs to improve VM performance while reducing processing load on the Windows Hypervisor.

New Hyper-V VMs will also consume less power by virtue of the new Core Parking feature implemented into Windows Server 2008 R2. For detailed information on core parking, please see the “Reduced Multicore Power Consumption” section further down in this guide.

### 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. Three key examples are the new VM Chimney (also called TCP Offload), support for Jumbo Frames and new support for the Virtual Machine Queue (VMQ).

VM Chimney allows a VM to dump its network processing load onto the NIC of the host computer. This works the same as in a physical TCP Offload scenario, Hyper-V now simply extends this functionality into the virtual world. This benefits both CPU and overall network throughput performance, and it’s fully supported by Live Migration.

VM Chimney is disabled by default in Windows Server 2008 R2, Combined with compatible hardware, currently including vendors like Intel, VM Chimney significantly reduces the host server’s CPU burden when dealing with VM network traffic. This translates into better host system performance and a simultaneous boost to VM network throughput.

Like TCP Offloading, 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 essentially allows the host’s single NIC card to appear as multiple NICs to the VMs by allowing 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. The result is less data in the host’s buffers and an overall performance improvement to I/O operations.

## Terminal Services Becomes Remote Desktop Services for Improved Presentation 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 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.

Remote Desktop Services in Windows Server 2008 R2 covers the same basic technology features as did Terminal Services, so this name change necessarily filters down as well. The table below summarizes the new names for TS-to-RDS technologies in R2.

Table 2: New Remote Desktop Services Names for Corresponding Terminal Services Names

|  |  |
| --- | --- |
| **Terminal Services name** | **Remote Desktop Services name** |
| **Terminal Services** | Remote Desktop Services |
| **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 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 partners, which include Citrix, Unisys, HP, Quest, Ericom and several others. 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 Vista® 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. VDI addresses all these challenges with the following features:

**Improved User Experience**

For both VDI and traditional remote desktop services the quality of user experience is more important than ever before. The version of VDI and remote desktop services in Windows Server 2008 improves the end user experience through new Remote Desktop Protocol capabilities. These new capabilities, enabled with Windows Server 2008 R2 in combination with Windows® 7, help make the user experience for remote users almost identical to local users.

**Adds Remote Desktop Connection Broker to enable VDI.** The in-box Remote Desktop connection broker 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. Besides RDS, Microsoft VDI leverages the following technologies to provide a comprehensive solution:

* Hyper-V
* Live Migration
* System Center products including System Center Virtual Machine Manager 2008
* Microsoft Application Virtualization in Microsoft Desktop Optimization Pack (MDOP).

For comprehensive and cost-effective licensing of the above VDI infrastructure and management components a new packaged VDI offering, the Microsoft VDI Suite, will be available in Q4 of 2009. Additionally, a Windows Virtual Enterprise Centralized Desktop (VECD) license is required for each device accessing the VDI image, irrespective of the virtualization vendor.

**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:

* **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.
* **Improved integration with Windows 7 user interface**. Once accessed, RAD-delivered programs and desktops show up in the Start Menu 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.

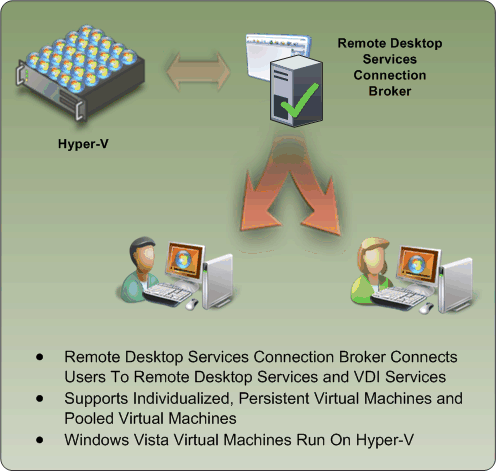


Figure 13: Remote Desktop Services Connection Broker

**Improving 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:

* **Windows Media® Redirection**: Provides high-fidelity multimedia by redirecting Windows media 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 16 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**: Supports any microphone connected to a user’s local machine. It enables audio recording support and speech recognition for RemoteApp and Remote Desktop.
* **Aero® Glass support**: 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 redirection**: 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.

While RDS improves the end-user experience, it 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 RDS 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 Windows 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.

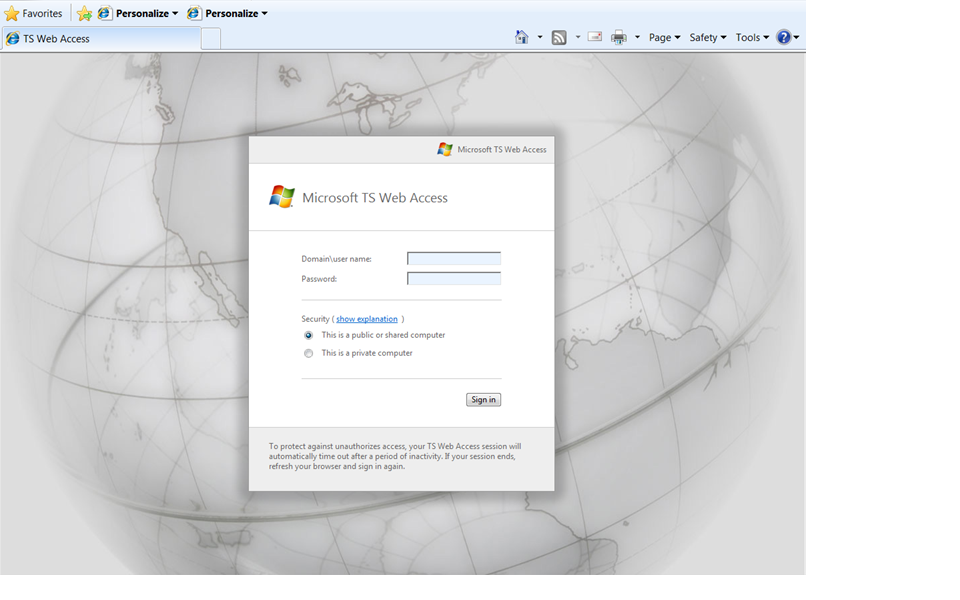
****

Figure 14: Remote Desktop Web Access expands RDS features cross-OS

Administrators faced with larger remote desktop 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 emerging VDI scenarios available via RDS. 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.** RD Gateway securely provides access to RDS resources from the Internet without the need for opening additional ports or the use of a VPN. RD Gateway provides this by tunneling RDP over HTTPS and incorporating several new security features:
* **Silent Session Re-authentication.** The Gateway administrator can now configure the RD Gateway 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 built RDS-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.
* **Connection broker extensibility.**  The connection 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.

# Management

The ongoing management of servers in the data center is one of most time-consuming task facing IT professionals today. Any management strategy you deploy must support the management of both your physical and virtual environments.

Another design goal for Windows Server® 2008 R2 is to reduce the ongoing management of Windows Server 2008 R2 and to reduce the administrative effort for common day-to-day operational tasks. These administrative tasks can be performed on the server or remotely.

Management improvements in Windows Server 2008 R2 include:

* 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, and
* 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.

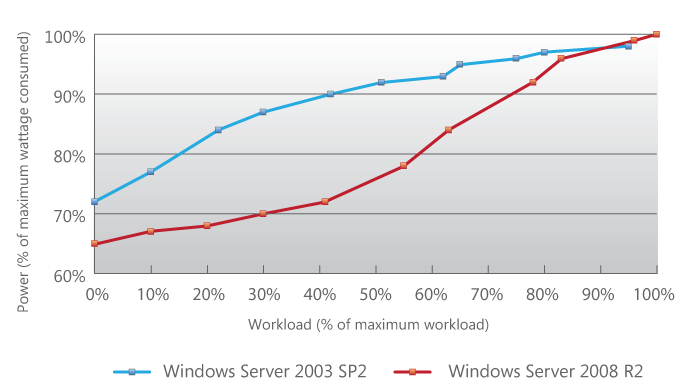


Figure 15 Power savings with Windows Server 2008 R2

### 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 16. 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](http://technet.microsoft.com/en-us/library/8677726a-2904-4074-9e89-7c965d63fdab), 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.

## Improved 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 introduces a number of improvements in remote administration, including the following:

* **Improved 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 offers a number of improvements for remote management scenarios. These improvements allow you to run scripts on one or more remote computers or to 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

Reducing administrative effort for day-to-day administrative tasks is another key design goal for Windows Server 2008 R2. Many of the management consoles used to manage Windows Server 2008 R2 have been updated or completely redesigned to help reduce your administrative effort. Some of the prominent updated and redesigned management consoles are listed in the following table with descriptions of the improvements.

Table 3: Updated & Redesigned Management Consoles in Windows Server 2008 R2

|  |  |
| --- | --- |
| **Management Console** | **Improvements** |
| **Server Manager** | * Support for remote management of computers * Improved integration with many role and role services management consoles |
| **Active Directory Administrative Center** | * Based on administrative capabilities provided by Windows PowerShell cmdlets * Task-driven user interface |
| **Internet Information Services** | * 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. |

## Enhanced Command-line and Automated Management

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

* **Improved remote management by using Windows PowerShell remoting**. For more information about Windows PowerShell remoting, see “Improved Remote Management” under “Management” in the upcoming Windows Server 2008 R2 Technical Overview.
* **Improved security for management data, including state and configuration information, by using constrained runspaces**. For more information about constrained runspaces, see “Improved Security for Management” under “Management” in the upcoming Windows Server 2008 R2 Technical Overview.
* **Enhanced GUIs for creating and debugging Windows PowerShell scripts and viewing PowerShell script output by using Graphical PowerShell and the Out-GridView cmdlet**. For more information about Graphical PowerShell and the Out-GridView cmdlet, see “Enhanced Graphical User Interfaces” under “Management” in the upcoming Windows Server 2008 R2 Technical Overview.
* **Extended scripting functionality that supports creation of more powerful scripts with less development effort**. For more information on this topic, see “Extended Scripting Functionality” under “Management” in the upcoming Windows Server 2008 R2 Technical Overview.
* **Improved portability of Windows PowerShell scripts and cmdlets between multiple computers**. For more information about this topic, see “Improved Portability of PowerShell Scripts and Cmdlets” under “Management” in the upcoming Windows Server 2008 R2 Technical Overview.

During your review of Windows PowerShell version 2.0 in Windows Server 2008 R2, you will want to familiarize yourself with the new GUI tools, Graphical PowerShell and the **Out-GridView** cmdlet. As illustrated in the following figure, Graphical PowerShell provides a GUI that allows you to interactively create and debug Windows PowerShell scripts within an integrated development environment similar to Microsoft Visual Studio®.

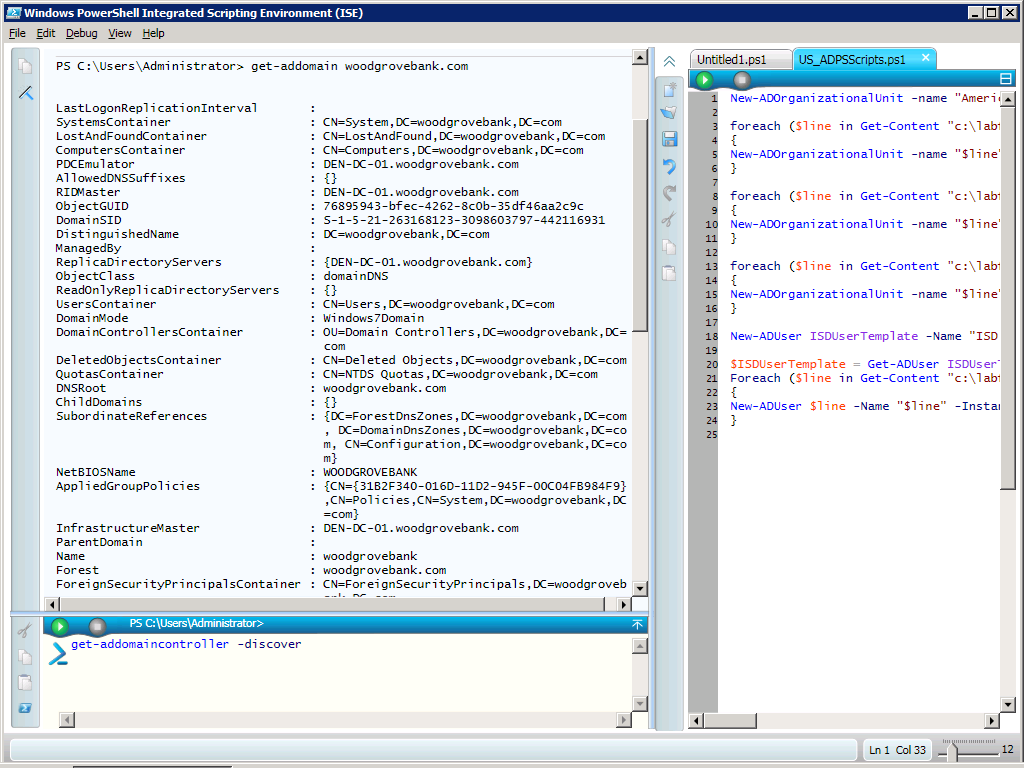


Figure 17: Graphical PowerShell user interface with Active Directory Provider

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 of a script, within the integrated development environment
* Support for up to eight Windows PowerShell runspaces within the integrated development environment

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

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:** The **Out-GridView** cmdlet feature requires Microsoft .NET Framework 3.0.

Also during your review, you will want to familiarize yourself with the new and updated cmdlets available in Windows PowerShell version 2.0 and Windows Server 2008 R2, a very few of which are listed in the following figure.



Figure 18: A snapshot of new cmdlets

## 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 managed system are one of the largest security concerns for any organization.

Windows Server 2008 R2 includes identity management improvements in the Active Directory 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.
* **Improved automated monitoring and notification**. An updated System Center Manager 2007 Management Pack helps improve the monitoring and management of Active Directory server roles.

#### Active Directory PowerShell Cmdlets: Step-by-step Feature Review

In this task you will use the PowerShell V2 Graphical Console to perform basic user and group administrative tasks. You will begin by loading the ActiveDirectory module, exposing over 75 Active Directory cmdlets. You will then use these cmdlets to administer Active Directory Domain Services (AD  DS).

To review how the Active Directory PowerShell cmdlets feature works, you need to complete the tasks in the following table. Perform the steps in the following table while logged on as a member of the Enterprise Admins security group.

Table 4: Active Directory PowerShell Cmdlets

|  |  |
| --- | --- |
| **High-level task** | **Details** |
| **Start the PowerShell V2 Graphical Console** | 1. On the Start menu, click **All Programs**, click **Windows PowerShell V2**, and then click **Graphical Console (Windows PowerShell V2)**. |
| **Load the Active Directory Module** | 1. In the PowerShell V2 Graphical Console, in the **Command Pane**, type the following commands, pressing **Enter** after each command.   Add-Module ActiveDirectory  Get-Module |
| **List the available cmdlets** | 1. In the PowerShell V2 Graphical Console, in the **Command Pane**, type the following command, and then press **Enter**.   Get-Command \*ad\* |
| **Browse an Active Directory domain** | 1. In the Command Pane, enter the following commands, pressing **Enter** after each command (where domain\_name is the name of your domain and top\_level\_domain is your top level domain).   Cd AD:  PWD  DIR | Format-Table -Auto  CD "DC=***domain\_name***,\_name DC=***top\_level\_doman***"  DIR | ft –a  **Tip:** You can press the TAB key to auto complete many of these commands and save a great deal of typing. |
| **List all user objects** | 1. In the Command Pane, enter the following commands, pressing **Enter** after each command.   CD CN=Users  Dir | ft –a  Get-ADObject –Filter {name -like “\*”}  Get-ADUser –Filter {name -like “\*”}  Get-ADUser -Filter {name -like "\*"} | Select Name, Enabled | Format-Table -Auto |
| **Enable the Guest user object** | 1. In the Command Pane, enter the following commands, pressing **Enter** after each command.   Enable-ADAccount –Identity Guest  Get-ADUser -Filter {name -like "\*"} | Select Name, Enabled | Format-Table -Auto |
| **Display information about the Domain Admins group** | 1. In the Command Pane, enter the following commands, pressing **Enter** after each command (where domain\_name is the name of your domain and top\_level\_domain is your top level domain).   Get-ADGroup -SearchBase "DC=***domain\_name***,DC=***top\_level\_domain***" -SearchScope Subtree -Filter {Name -Like "\*Domain Admins\*"} -Properties Extended |
| **Display information about a domain** | 1. In the Command Pane, type the following command and then press **Enter** (where domain\_name is the name of your domain).   Get-ADDomain ***domain\_name***  The output of this command allows you to easily determine things such as operations master roles. |
| **Display information about domain controllers** | 1. In the Command Pane, type the following command and then press **Enter**.   Get-ADDomainController –Discover |
| **Display information about the domain password policy** | 1. In the Command Pane, type the following command and then press **Enter** (where domain\_name is the fully qualified domain name of your domain).   Get-ADDefaultDomainPasswordPolicy ***domain\_name*** |
| **Create a new organizational unit** | 1. In the Command Pane, type the following command and then press **Enter** (where where domain\_name is the name of your domain and top\_level\_domain is your top level domain).   New-ADOrganizationalUnit –Name “Europe” –Path “DC=***domain\_name***,DC=***top\_level\_domain***” |
| **Display the properties of the new organizational unit** | 1. In the Command Pane, type the following command and then press **Enter** (where where domain\_name is the name of your domain and top\_level\_domain is your top level domain).   Get-ADOrganizationalUnit “OU=Europe,DC=***domain\_name***,DC=***top\_level\_domain***” –Properties Extended |
| **Delete the new organizational unit** | 1. In the Command Pane, type the following commands and then press **Enter** after each command (where where domain\_name is the name of your domain and top\_level\_domain is your top level domain).   CD AD:  CD “DC=***domain\_name***,DC=***top\_level\_domain***”  Set-ADorganizationalUnit Europe –ProtectedFromAccidentalDeletion $False  Remove-ADOrganizationalUnit Europe |
| **Close the PowerShell V2 Graphical Console** | 1. Close the PowerShell V2 Graphical Console. |

### Improvements in Active Directory Domain Services (AD DS)

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

* **Recovery of deleted objects**. Domains in AD DS 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. This feature requires the updated R2 forest functional level.
* **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 an XML 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 time-consuming management task is the maintenance of 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 also must be updated with the new password. To address this problem, Windows Server 2008 R2 includes a new feature known as 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 services that use the service account.
* **Reduced effort to perform common administrative tasks**. As illustrated in the following figure, Windows Server 2008 R2 includes a new Active Directory Domain Services management console, Active Directory Administrative Center.

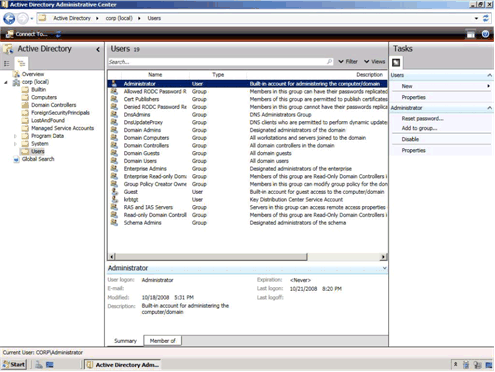


Figure 19: Active Directory Administrative Center management console

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.

#### Active Directory Administrative Center: Step-by-step Feature Review

To review how the Active Directory Administrative Center feature works, you need to complete the tasks in the following table. Perform the steps in the following table while logged on as a member of the Enterprise Admins security group.

Table 5: Explore the Active Directory Administrative Center

|  |  |
| --- | --- |
| **High-level task** | **Details** |
| **Start the Active Directory Administrative Center** | 1. On the Start menu, point to **Administrative Tools**, and then click **Active Directory Administrative Center**. |
| **Navigate to an organizational unit** | 1. In Active Directory Administrative Center, in the **Explorer** pane, click **Overview**. 2. Using the fly-out menu system, navigate to organizational\_unit (where organizational\_unit is the name of the organizational unit where you want to create an organizational unit).   **Tip:** Click the right arrow next to the domain root to begin using the fly-out menu system. As you navigate, type the first few letters of each organizational unit to shorten the navigation. |
| **Create an organizational unit** | 1. In the **Tasks** pane, click **New**, and then click **Organizational Unit**.   The Create dialog box appears.   1. In the **Create** dialog box, in **Name**, type **Demonstration OU**, and then click **OK**. |
| **Create a user** | 1. Using the fly-out menu system, navigate to **Demonstration OU**. 2. In the **Tasks** pane, click **New**, and then click **User**.   The Create dialog box appears.   1. Compete the **Create** dialog box by using the following information, and then click **OK**:  * First Name: **Pilar** * Last Name: **Ackerman** * User logon: **pilarau** * Select **Password never expires** check box. * Clear **Change password at next logon** check box. * Password: **P@ssw0rd** |
| **Create a new group** | 1. Using the fly-out menu system, navigate to **Demonstration OU**. 2. In the **Tasks** pane, click **New**, and then click **Group**.   The Create dialog box appears.   1. Compete the **Create** dialog box by using the following information, and then click **OK**:  * Name: **Support** * Select **Protect from Accidental Deletion** check box. |
| **Add a user to a group** | 1. In **Search**, type **Pilar Ackerman**. 2. In the **Results** pane, click **Pilar Ackerman**. 3. In the **Tasks** pane, click **Add to group**. 4. In the **Select Groups** dialog box, in **Enter the object names to select**, type **Support**, click **Check Names**, and then click **OK**. |

#### Active Directory Recycle Bin: Step-by-step Feature Review

To review how the Active Directory Recycle Bin feature works, you need to complete the following tasks:

1. Enable the Active Directory Recycle Bin feature.
2. Delete objects in AD DS.
3. Verify the deleted objects are in the Active Directory Recycle Bin.
4. Recover the objects in the Active Directory Recycle Bin.
5. Verify the deleted objects have been recovered.

**Note:** Perform these steps in a test environment as these steps could adversely affect your production environment.

##### Enable the Active Directory Recycle Bin Feature

Perform the steps in the following table while logged on as a member of the Enterprise Admins security group. Before you can recover deleted objects in your Active Directory infrastructure, you must enable the Active Directory Recycle Bin feature.

Table 6: Enable the Active Directory Recycle Bin Feature

|  |  |
| --- | --- |
| **High-level task** | **Details** |
| **Start the Active Directory PowerShell Snap-in** | 1. On the Start menu, point to **Administrative Tools**, and then click **Active Directory PowerShell Snap-in**. |
| **Check the state of the Recycle Bin feature** | 1. In Windows PowerShell, type the following command and then press **Enter**.   Get-ADOptionalFeature –Filter ‘Name –Like “\*”’  In the output you should see the:   * **EnabledScopes** property is currently empty, which indicates that this feature is not enabled. * **RequiredForestMode** property indicates the prerequisites for enabling this feature. |
| **Enable the Recycle Bin feature** | 1. In Windows PowerShell, type the following command and then press **Enter** (where forest is the name of your forest).   Enable-ADOptionalFeature ‘Recycle Bin Feature’ –Scope Forest –Target ‘***forest***’  **Note:** The Recycle Bin feature is disabled by default.   1. To confirm the command, press **Enter**.   **Note:** Once you enabled the Recycle Bin feature, you cannot disable the feature at a later time. |
| **Verify the Recycle Bin feature is enabled** | 1. In Windows PowerShell, type the following command and then press **Enter**.   Get-ADOptionalFeature –Filter ‘Name –Like “\*”’  The value of the EnabledScopes property reflects that the Recycle Bin is enabled. |

##### Delete Objects in AD DS

Perform the steps in the following table while logged on as a member of the Enterprise Admins security group.

Table 7: Delete Objects in AD DS

|  |  |
| --- | --- |
| **High-level task** | **Details** |
| **Start the Active Directory Administrative Center** | 1. On the Start menu, point to **Administrative Tools**, and then click **Active Directory Administrative Center**. |
| **Navigate to an organizational unit** | 1. Using the fly-out menu system, navigate to Demonstration OU   **Tip:** Click the right arrow next to the domain root to begin using the fly-out menu system. As you navigate, type the first few letters of each organizational unit to shorten the navigation. |
| **Delete an organizational unit** | 1. In the **Tasks** pane, click **Delete**. 2. In the **Delete Confirmation** dialog box, click **Yes**. |

##### Verify the deleted objects are in the Active Directory Recycle Bin

Perform the steps in the following table while logged on as a member of the Enterprise Admins security group.

Table 8: Verify the deleted objects are in the Active Directory Recycle Bin

|  |  |
| --- | --- |
| **High-level task** | **Details** |
| **Start the Active Directory PowerShell Snap-in** | 1. On the Start menu, point to **Administrative Tools**, and then click **Active Directory PowerShell Snap-in**. |
| **Display the contents of the Recycle Bin** | 1. In Windows PowerShell, type the following command and then press **Enter** (where domain is your domain name and top\_level\_domain is your top level domain name).   Get-ADObject –SearchBase “CN=Deleted Objects,DC=***domain***,DC=***top\_level\_domain***” –ldapFilter “(objectClass=\*)” -includeDeletedObjects  This command displays the entire contents of the recycle bin.   1. Leave the output of this command on the screen as you will use it in the next step. |
| **Verify the Pilar Ackerman user object is in the Recycle Bin** | 1. In Windows PowerShell, type the following command and then press **Enter**.   Get-ADObject –Filter ‘Name –Like “\*Pilar Ackerman\*”’ –SearchScope Subtree –includeDeletedObjects  The output of this command will show the details for the Pilar Ackerman user object. The distinguished name indicates this object is in the Recycle Bin. |
| **Verify the Demonstration OU is in the Recycle Bin** | 1. In Windows PowerShell, type the following command and then press **Enter**.   Get-ADObject –Filter ‘Name –Like “\*Demonstration OU\*”’ –SearchScope Subtree –IncludeDeletedObjects  The output of this command will show the details for the Demonstration OU organizational unit. The distinguished name indicates this object is in the Recycle Bin. |

##### Recover Deleted Objects in Active Directory Recycle Bin

Perform the steps in the following table while logged on as a member of the Enterprise Admins security group.

Table 9: Recover Deleted Objects in Active Directory Recycle Bin

|  |  |  |
| --- | --- | --- |
| **High-level task** | **Details** | |
| **Start the Active Directory PowerShell Snap-in** | | 1. On the Start menu, point to **Administrative Tools**, and then click **Active Directory PowerShell Snap-in**. |
| **Attempt to restore the Pilar Ackerman user object** | 1. In Windows PowerShell, copy the **objectGUID** value for the object Pilar Ackerman to the clipboard.   **Tip:** To copy text from a command prompt, right click and then select Mark. Highlight the text to copy and then press Enter. The objectGUID was listed in a previous output.   1. In Windows PowerShell, type the following command and then press **Enter** (where objectGUID is the objectGUID for Pilar Ackerman).   Restore-ADObject –Identity **objectGUID**  **Tip:** To paste, right-click and then click Paste.   1. The command fails with an error message indicating that the objects parent object does not exist. | |
| **Identify the parent container for the Pilar Ackerman user object** | 1. In Windows PowerShell, type the following command and then press **Enter**.   Get-ADObject –Filter ‘Name –Like “\*Pilar Ackerman\*”’ –SearchScope Subtree –includeDeletedObjects –properties lastKnownParent  This command displays the last known parent object, which you can tell, is also in the Recycle Bin. | |
| **Restore the deleted organizational unit** | 1. In Windows PowerShell, type the following command and then press **Enter** (where *objectGUID* is the objectGUID of the Demonstration OU organizational unit).   Restore-ADObject –Identity objectGUID  **Tip:** To complete this command, copy the value of the objectGUID property from the Demonstration OU object, which can be found from the output of the last command. | |
| **To restore all the deleted objects** | 1. In Windows PowerShell, type the following command and then press **Enter** (where domain is your domain name and top\_level\_domain is your top level domain name). 2. Get-ADObject –ldapFilter “(lastKnownParent=OU=Demonstration OU, DC=domain,DC=top\_level\_domain)” –includeDeletedObjects | Restore-ADObject   This command lists all objects that have the last known parent attribute as the Demonstrated OU and pipes them into the Restore-ADObject Cmdlet. | |

##### Verify the Deleted Objects Are Recovered

Perform the steps in the following table while logged on as a member of the Enterprise Admins security group.

Table 10: Verify the Deleted Objects Are Recovered

|  |  |
| --- | --- |
| **High-level task** | **Details** |
| **Start the Active Directory Administrative Center** | 1. On the Start menu, point to **Administrative Tools**, and then click **Active Directory Administrative Center**. |
| **Verify the Demonstration OU organizational unit has been recovered** | 1. Using the fly-out menu system, navigate to Demonstration OU   **Tip:** Click the right arrow next to the domain root to begin using the fly-out menu system. As you navigate, type the first few letters of each organizational unit to shorten the navigation. |
| **Verify the Pilar Ackerman user object has been recovered** | 1. In **Search**, type **Pilar Ackerman**   The Pilar Ackerman user object should appear in the results pane. |

#### Offline Domain Join: Step-by-step Feature Review

Offline domain join involves two steps. In the first step you provision a computer account in AD DS and save the account information in a file. In the second step you use that file in a command that inserts the domain join information into an offline version of Windows.

Perform the steps in the following table while logged on as a member of the Enterprise Admins security group.

Table 11: Offline domain join

|  |  |
| --- | --- |
| **High-level task** | **Details** |
| **Provision a new computer account** | 1. On the Start menu, in **Start Search**, type cmd, and then press **Enter**. 2. At the command prompt, type the following command and then press **Enter** (where domain\_name is the name of your domain).   DJOIN /Provision /Domain domain\_name /Machine DEN-SRV-01 /SaveFile DEN-SRV-01.DJoin  This command creates a computer account in Active Directory and stores the computer account password and related information in an encrypted file. The encrypted file can then be used to offline domain join a computer. |
| **Display the contents of the provisioning file** | 1. At the command prompt, type the following command and then press **Enter**.   Type DEN-SRV-01.DJoin  **Note:** The contents of the .DJoin file are encrypted. |
| **Verify the computer account is created in Active Directory** | 1. On the Start menu, point to **Administrative Tools** and then click **Active Directory Administrative Center**. 2. Using the fly-out menu system, navigate to domain\_name**\Computers** (where domain is the name of your domain).   **Tip:** Click the right arrow next to the domain root to begin using the fly-out menu system. As you navigate, type the first few letters of each organizational unit to shorten the navigation.   1. In the information pane, note that the computer account DEN-SVR-01 has been created. |
| **To join the computer to the domain** | 1. The following command would be run on DEN-SRV-01 to join that computer to the domain   DJOIN /Requestodj /LoadFile DEN-SVR-01.DJoin /WindowsPath \Mount\Windows  **Note:** Do not run this command. It is provided for reference purposes only.  This command is intended to be run against an offline copy of Windows such as a WIM file or VHD that has been mounted as a drive or folder in the file system. |

### Improvements in Active Directory Federated Services

Active Directory Federated Services in Windows Server 2008 R2 includes a new feature known as authentication assurance. This feature allows administrators to establish authentication policies for accounts that are authenticated in federated domains. This enables a variety of advanced authentication scenarios, such as smart cards, for example.

## Improved Compliance with Established Standards and Best Practices

Windows Server 2008 R2 includes an integrated Best Practices Analyzer for each of the server roles. The Best Practices Analyzer creates a checklist within Server Manager for the role, which you can use to help perform all the configuration tasks.

# 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 Windows 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 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 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.

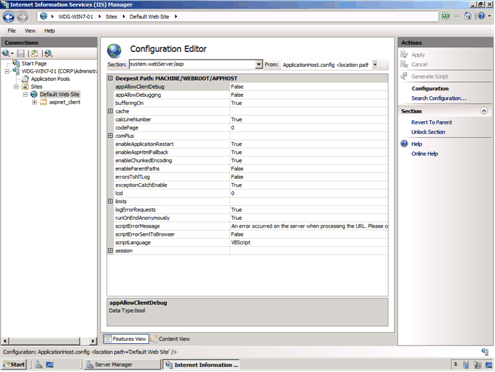


Figure 20: Configuration Editor user interface

##### 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.

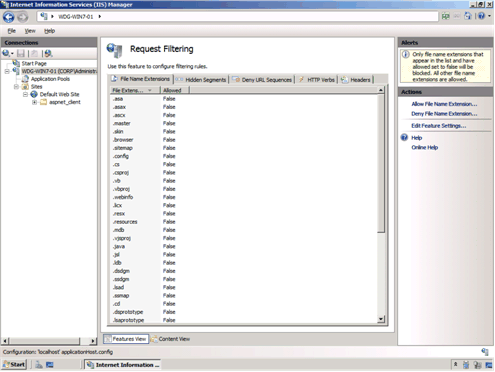


Figure 21: Request Filtering user interface

#### 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.

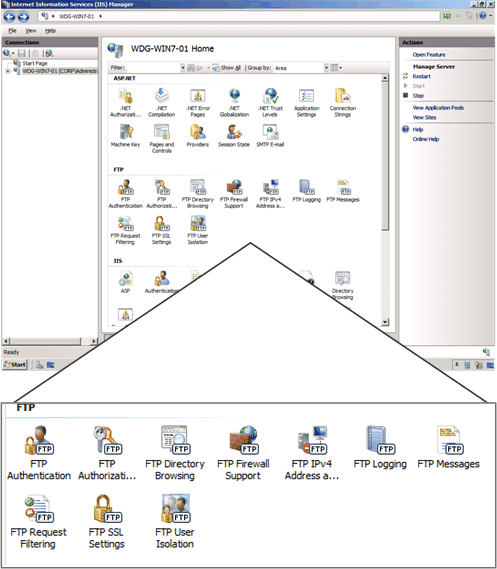


Figure 22: Integration of the FTP server administration in Internet Information Service Manager

* **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.

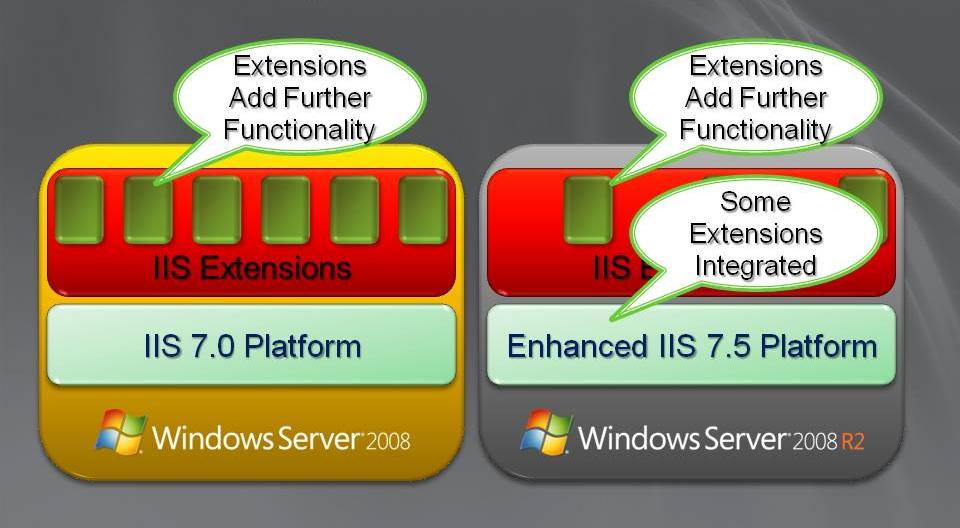


Figure 23: Architecture of IIS Extensions in IIS 7.5 in Windows Server 2008 R2

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 a best-of-breed enterprise operating platform, capable of handling the most demanding data center workloads and delivering the latest next-gen network productivity experience to end-users across even the largest networks. To address these challenges, Microsoft has designed Windows Server 2008 R2 with several new feature categories in mind, divisible into two basic categories:

* Scalability and Reliability
* Better Together with Windows® 7.

## Scalability and Reliability

Windows Server 2008 R2 is capable of the unprecedented workload size, dynamic scalability and across-the-board availability and reliability. A host of new and updated features contribute to this pillar:

* Leveraging sophisticated CPU architectures
* Increased operating system componentization
* Improved performance and scalability for applications and services

### Leveraging Sophisticated CPU Architectures

Windows Server 2008 R2 is the first Windows operating system to be offered for only 64-bit processors. With customers being unable to purchase a 32-bit server CPU for over two years, the performance and reliability advantages to moving to this architecture were too beneficial to ignore.

Additionally, Windows Server 2008 R2 now supports up to 256 logical processor cores for a single operating system instance. Hyper-V™ is able to utilize up to 64 logical cores on a single host. These improvements not only guarantee more bang for your server hardware buck, but also offer better reliability with fewer locks and greater parallelism.

### Increased Operating System Componentization

Microsoft introduced the concept of server roles to allow server administrators to quickly and easily configure any Windows-based server to run a specific set of tasks and remove extraneous OS code from system overhead. Windows Server 2008 R2 further extends this model with support for more roles and a broadening of current role support, like the addition of ASP.NET within IIS 7.5.

Roles have been refined and feature sets redefined as customers have expressed desires for certain capabilities in popular scenarios. The Server Core installation option is an appropriate mention here with new (and much demanded) support for Windows PowerShell™ scripting made possible by the addition of the .NET Framework to the list of server roles supported in the Server Core installation option.

### 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. Windows Server 2008 R2 features that improve performance and scalability for applications and services include:

* Support for larger workloads by adding more 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 NLB to distribute workloads across the cluster nodes in order to support a larger number of simultaneous users. Network Load Balancing feature improvements in Windows Server 2008 R2 include:

* Improved support for applications and services that require persistent connections.
* 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

As illustrated in the following figure, 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 be maintained with a specific cluster node.

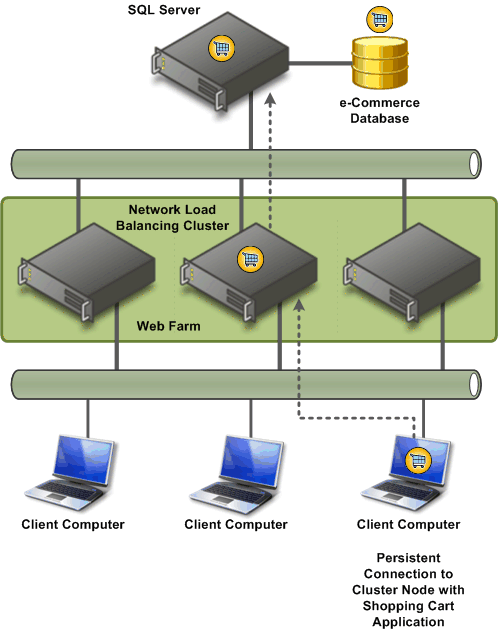


Figure 24: IP Stickiness feature in Network Load Balancing

You can configure a time-out 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), which uses an SSL–based virtual private network (VPN).
* Web-based applications that maintain user information, such as an ASP.NET shopping cart application.

##### Improved Health Monitoring and Awareness for Applications and Services

As illustrated in the following figure, 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.

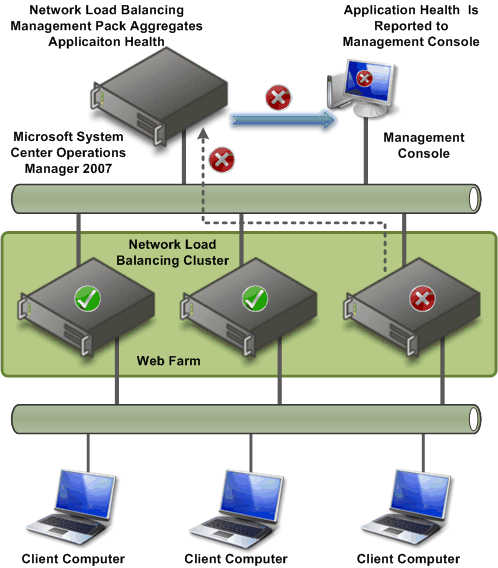


Figure 25: Application health monitoring in Network Load Balancing clusters

#### 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 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 iSCSI and other remote storage solutions. For more information on these improvements in storage device performance, see “Improved File Services and Network Attached Storage” later in this guide.

### 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 (NAS). Microsoft storage solutions are at the core of providing high-performance and highly available file services and NAS.

The release version of Windows Server 2008 introduced many improvements in storage technologies. Windows Server 2008 R2 includes additional improvements that enhance 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:

* **Reduced processor utilization to achieve “wire speed” storage performance**. *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/output process performance**. One of the primary contributors to storage performance improvements in Windows Server 2008 R2 is the improvement in the storage input/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 performance for iSCSI attached storage.
* **Improved support for optimization of the 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 were not shut down 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 the 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 to quickly restore to a previous version in the event of a configuration error.

### 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 anti-virus 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

Storage is no longer a marginal expense. Nor is managing storage any longer simply about volume and availability; organizations need to manage their data more effectively as well as more efficiently. Only by gaining insight into their data can companies reduce the cost of storing, maintaining, and managing data. Only by enforcing company policies and knowing how storage is utilized can administrators efficiently use their storage and mitigate the risks of leaking data. The next frontier for administrators is to be able to manage data based on business value.

Windows Server 2008 R2 File Classification Infrastructure (FCI) provides insight into your data by automating classification processes so that you can manage your data more effectively and economically. FCI does this by enabling to automatically classify files based on properties defined by administrators (such as whether or not a file contains personally identifiable information) and performing administrator-specified actions based on that classification (backing up files containing personal information to an encrypted store, for example). These mechanisms are included in the box as well as provided by partner interfaces that allow IT organizations and partners to build rich end to end solutions for classifying and applying policy based on classification. FCI helps customers save money and reduce risk by managing files based on their business value and business impact.

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 in the box

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.

With no additional third-party applications, FCI provides the following benefits:

* **Getting insight to data on file server** —Administrators can create automatic classification rules that classify files according to the location or content of the files. As a result, a new layer of efficiency is added, driving down the typical costs associated with managing and protecting the file server.
* **Reduce storage costs and eliminate old documents with no business value** — Storing stale, unused data can grow to be a major expense for organizations. Indeed, IDC estimates that 60-80 percent of file data has no legal or business value. Expiring files based on usage and business value can reduce both the cost (storage and management) and risk (information leakage) on file servers. The in-box FCI solution provides automatically scheduled tasks that expire files based on age, location, or other classification categories.
* **Mitigate risk by customizing how and where your data is stored** — FCI empowers administrators to run custom commands that automate management tasks based on file name, age, location, or other classification categories of files. For example, IT administrators can automatically move data based on policies for either centralizing the location of sensitive data or for moving data to a less expensive storage facility.
* **Easily track files** — Reports can provide administrators with a powerful tool to assess the risk of the wrong files being in the wrong place on their servers. Using the built-in capabilities of FCI, administrators can create reports in a variety of formats that contain details—including location—about files that have a particular classification. The FCI reporting infrastructure can also be used to generate information that can be used by another application.

#### 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 Development of File Management Tasks

There are many solutions on the market that provide data management and solutions that classify and protect information, each dealing with specific aspects of the challenges presented by data growth. FCI provides an extensible infrastructure to allow these solutions to work with one another and empower companies to craft rich, end-to-end data-management solutions that meet their specific business objectives. FCI persists file classification between different ISV offerings so that products that classify files can work with products that consume file classifications. For example, if a data leakage–prevention product classifies files as containing personal information, then a backup product can back it up to an encrypted store rather than the regular store. Moreover, IT administrators can build in-house solutions that plug into the classification infrastructure and interoperate with ISV product offerings.

### 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 back up an 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 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 12: 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 13: 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 follow is the sequence of events when performing a full volume restore using LUN synchronization:

The source and destination LUNs are identified.

1. The LUN resynchronization is initiated between the source (shadow copy) and destination LUNs.
2. 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.

1. The LUN resynchronization continues by performing a block-level copy from the source (shadow copy) LUN to the destination LUN.
2. 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 specifically to work with client computers running Windows 7, the next version of the Windows operating system from Microsoft. Features that are only available when 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 BranchCache feature
* Improved security for branch offices by using the read-only Distributed File System (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 RemoteApp and Desktop Connections 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 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 common problem facing most organizations is remote connectivity for their mobile users. One of the most widely used solutions for remote connectivity is for mobile users to connect by using a virtual private network (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 in Windows Server 2008 R2 allows Windows 7 client computers 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 that they are remotely connecting to intranet resources. The following figure contrasts the current VPN-based solutions with DirectAccess–based solutions.

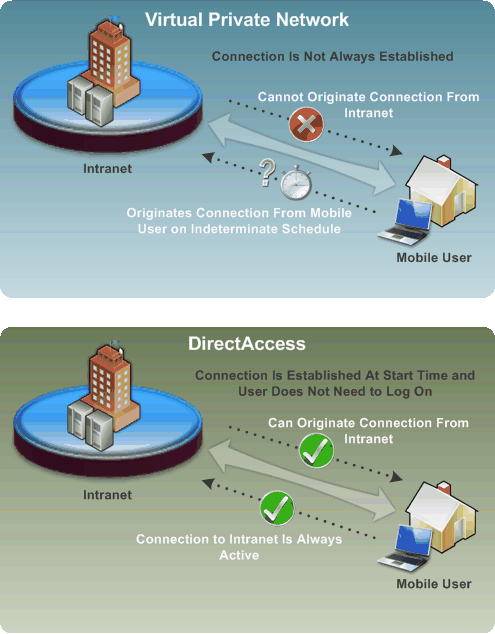


Figure 26: Comparison between VPN-based and DirectAccess–based solutions

DirectAccess was designed ground-up to manage a user-invisible always-on remote access solution that removes all user complexity, gives you easy and efficient management and configuration tools and doesn’t compromise in any way the security aspect of remote connectivity. To do this, Windows Server 2008 R2’s DirectAcces incorporates the following important features:

* **Authentication.** DirectAccess authenticates the computer, enabling the computer to connect to the intranet before the user logs on. DirectAccess can also authenticate the user and supports multifactor authentication such as a smart card.
* **Encryption.** DirectAccess uses IPsec for encrypted communications across the Internet.
* **Access control.** IT can configure which intranet resources different users can access using DirectAccess. IT can grant DirectAccess users unlimited access to the intranet, or only allow them to access specific servers or networks.
* **Integration with Network Access Protection (NAP) and Network Policy Server (NPS).** NAP and NPS, features built into Windows Server 2008 and Windows 7 Server, can verify that client computers meet your security requirements and have recent updates installed before allowing them to connect.
* **Split-tunnel routing.** Only traffic destined for your intranet is sent through the DirectAccess server. With a traditional VPN, Internet traffic is also sent through your intranet, slowing Internet access for users.

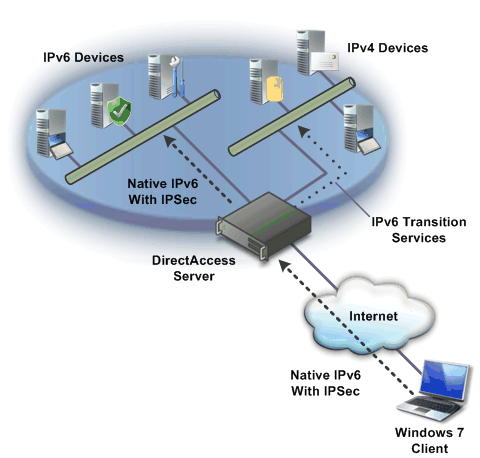


Figure 27: DirectAccess remote access solution

Unlike a traditional VPN-based solution, the DirectAccess client forwards traffic destined for Internet-based resources directly to the Internet-based resource. In a traditional VPN-based solution, all traffic, both Internet and intranet traffic, is sent through the VPN connection. Separating the Internet-based traffic from the intranet-based traffic helps reduce remote access network utilization.

Another difference between DirectAccess and VPNs is that DirectAccess connections are established before the user is logged in. This means that you can manage a remote computer connected by DirectAccess even if the user is not logged in; for example, to apply Group Policy settings. However, for the user to access any corporate resources, they must be logged in.

In order to benefit from DirectAccess, you must be able to access the resources within your intranet by using IPv6. If your organization has an IPv6 routable infrastructure, no IPv6 translation is required. If you have resources that only have IPv4 addressing, you will need to provide IPv6-to-IPv4 transition services.

The DirectAccess server supports the Teredo Server, Teredo Relay, ISATAP Router, NAT-PT and 6to4 router transition technologies. Additionally, the Microsoft Forefront™ Intelligent Access Gateway (IAG) solution will integrate with DirectAccess to provide additional management, security and deployment capabilities. This IAG solution will become available approximately 6 months after the launch of Windows Server 2008 R2 and the Windows 7 client.

### 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 the user’s 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 Gateway features allows users on Windows 7 clients to remotely access their intranet-based resources without requiring any additional software to be installed on the Windows 7 client. This allows your users to remotely access their desktop as though they were working from their computer on the intranet.

The following figure highlights some of the new features provided by Virtual Desktop Infrastructure (VDI) and Terminal Services in Windows Server 2008 R2. For more information on these features, see “Secured Remote Connectivity for Private and Public Computers” in “Better Together with Windows 7” in Windows Server 2008 R2 Technical Overview.

From the user’s perspective, the desktop on the remote Windows 7 client transforms to look like the user’s desktop on the intranet, including icons, Start menu items and installed applications are identical to the user’s experience on his or her own 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

Driven by challenges of reducing cost and complexity of Branch IT, organizations are seeking to centralize applications. However, as organizations centralize applications the dependency on the availability and quality of the WAN link increases. A direct result of centralization is the increased utilization of the WAN link, and the degradation of application performance. Recent studies have shown the despite of the reduction of costs associated with WAN links, and WAN costs are still a major component of enterprises’ operational expenses.

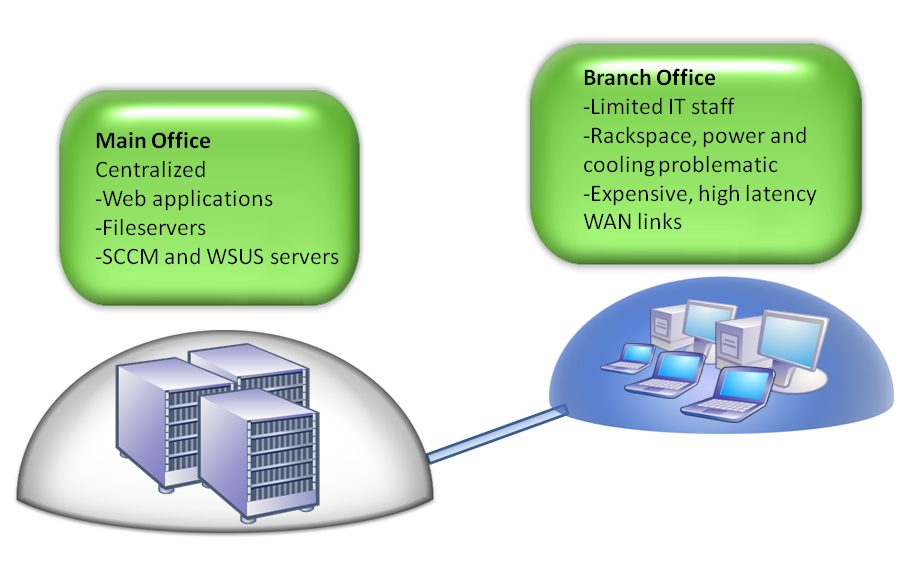


Figure 28: The branch office problem

The BranchCache feature in Windows Server 2008 R2 and Windows 7 Client reduces the network utilization on WAN links that connect branch offices and improve end user experience at branch locations, by locally caching frequently used content on the branch office network.

As remote branch clients attempt to retrieve data from servers located in the corporate data center, they store a copy of the retrieved content on the local branch office network. Subsequent requests for the same content are served from this local cache in the branch office, thereby improving access times locally and reducing WAN bandwidth utilization between the branch and corpnet. BranchCache caches both HTTP and SMB content and ensures access to only authorized users as the authorization process is carried out at the servers located in the data center. BranchCache works alongside SSL or IPSEC encrypted content and accelerates delivery of such content as well.

BranchCache can be implemented in two ways: The first involves storing the cached content on a dedicated BranchCache server located in the branch office which improves cache availability. This scenario will likely be the most popular and is intended for larger branch offices where numerous users might be looking to access the BranchCache feature simultaneously. A BranchCache server at the remote site ensures that content is always available as well as maintaining end-to-end security for all content requests.

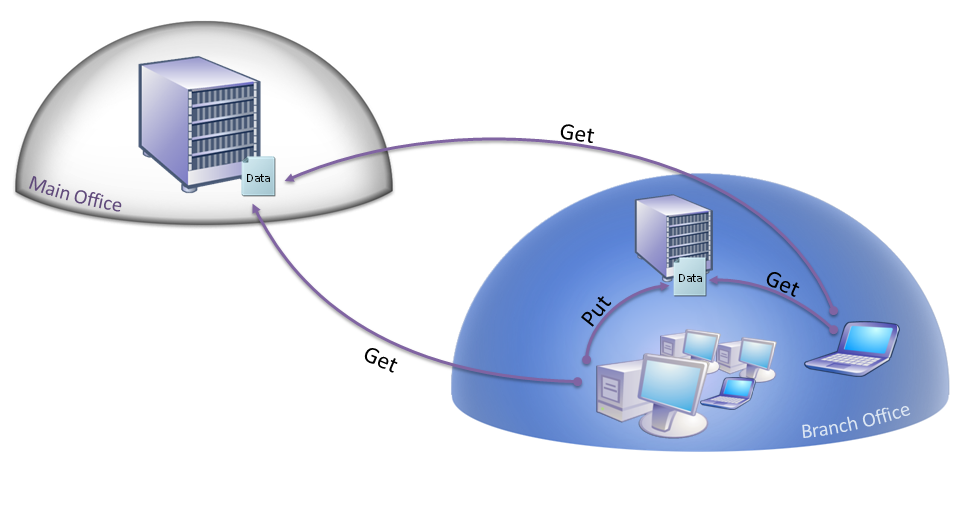


Figure 29: The BranchCache server deployment scenario

The second deployment scenario centers around peer content requests and is intended solely for very small remote offices, with roughly 5-10 users that don’t warrant a dedicated local server resource. In this scenario, the BranchCache server at corpnet receives a client content request, and if the content has been previously requested at the remote site will return a set of hash directions to the content’s location on the remote network, usually another worker’s PC. Content is then served from this location. If the content was never requested or if the user who previously requested the content is off-site, then the request is fulfilled normally across the WAN.

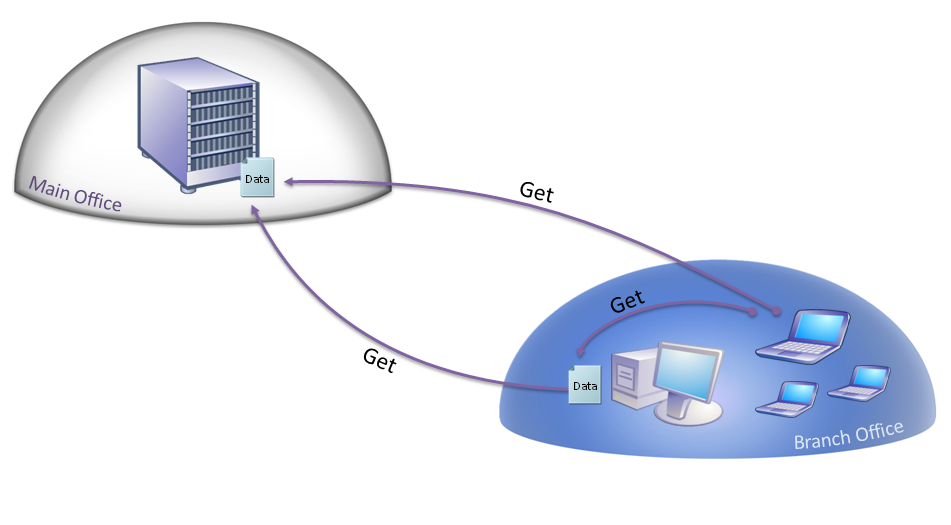


Figure 30: BranchCache peer-based deployment model

#### Hosted Caching for HTTP Content: Step-by-step Feature Review

To review how the Hosted Caching feature works for HTTP content, you need to complete the following tasks:

1. Configure the BranchCache feature to support caching of HTTP content.
2. Enable the BranchCache feature on client computers using Group Policy settings.
3. Verify the performance of HTTP content caching.

**Note:** Perform these steps in a test environment as these steps could adversely affect your production environment. Also, you need to have a method of simulating a Wide Area Network (WAN) connection to perform these steps.

##### Configure BranchCache Feature for HTTP Content Caching

Perform the steps in the following table while logged on as a member of the Enterprise Admins security group.

Table 14: Configure BranchCache Feature for HTTP Content Caching

|  |  |
| --- | --- |
| **High-level task** | **Details** |
| **Start Server Manager** | 1. On the Start menu, point to **Administrative Tools**, and then click **Server Manager**. |
| **Install the Windows Branch Cache feature** | 1. In Server Manager, click **Features**. 2. Under **Features Summary**, click **Add Features**. 3. In the **Add Features Wizard**, under **Features**, check **Windows Branch Cache**, click **Next**, and then click **Install**.   Wait for the installation to complete.   1. Click **Close**. |
| **Enable Hosted Cache Server mode** | 1. On the Start menu, in **Start Search**, type **cmd**, and then press **Enter**. 2. At the command prompt, type the following command and then press Enter.   netsh peerdist set service mode=HOSTEDSERVER |
| **Verify Hosted Cache Server mode is enabled** | 1. At the command prompt, type the following command and then press **Enter**.   Netsh peerdist show status all |
| **Verify SSL bindings** | 1. At the command prompt, type the following command and then press **Enter**.   Netsh http show sslcert  The SSL certificate mapping is required for the hosted cache to function. |
| **View the SSL certificate** | 1. At the command prompt, type the following command s, pressing **Enter** after each command.   PowerShell  CD Cert:  CD LocalMachine  CD MY  Get-ChildItem | Format-List \*  exit   1. View the value of the **Subject** field.   When configuring the hosted cache clients, you must use the computer name as listed in this field. |

##### Enable BranchCache Feature on Client Computers using Group Policy

Perform the steps in the following table while logged on as a member of the Enterprise Admins security group.

Table 15: Enable BrancheCache Feature using Group Policy

|  |  |
| --- | --- |
| **High-level task** | **Details** |
| **Start Group Policy Management console** | 1. On the Start menu, point to **Administrative Tools**, and then click **Group Policy Management.** |
| **Create new Group Policy object** | 1. In the Group Policy Management console, navigate to **forest\_name\Domains\domain\_name\Group Policy Objects**, right-click **Group Policy Objects**, and then click **New**. 2. In the **New GPO** dialog box, in **Name**, type **BranchCache Policy**, and then click **OK**. |
| **Configure BranchCache Group Policy settings** | 1. In the Group Policy Management console, right-click **BranchCache Policy**, and then click **Edit**.   The Group Policy Editor starts.   1. In the Group Policy Editor, go to **Computer Configuration/Policies/Administrative Templates: Policy definitions (ADMX files) retrieved from the local machine/Network/Windows Branch Cache**. 2. Configure the following settings (where server\_name is the fully qualified domain name of the server you are configuring):  * Turn on Windows Branch Cache: Enabled * Turn on Windows Branch Cache – Hosted cache mode: Enabled * Turn on Windows Branch Cache – Hosted cache mode: Cache Location: server\_name. |
| **Configure Windows Firewall Inbound Rules Group Policy settings for BrancheCache** | 1. In the Group Policy Editor, go to **Computer Configuration/Policies/Windows Settings/Security Settings/Windows Firewall with Advanced Security/Inbound Rules.** 2. On the **Action** menu, click **New Rule**. 3. Create a new inbound rule using the values in the following information.  * Rule Type: Predefined: Peer Distribution – HTTP Transport (Uses HTTP) * Action: Allow the connection  1. On the **Action** menu, click **New Rule**. 2. Create a new inbound rule using the values in the following information.  * Rule Type: Predefined: Peer Distribution – Hosted Cache (Uses HTTP) * Action: Allow the connection |
| **Configure Windows Firewall Inbound Rules Group Policy settings for BrancheCache** | 1. In the Group Policy Editor, go to **Computer Configuration/Policies/Windows Settings/Security Settings/Windows Firewall with Advanced Security/Outbound Rules.** 2. On the **Action** menu, click **New Rule**. 3. Create a new outbound rule using the values in the following information.  * Rule Type: Predefined: Peer Distribution – HTTP Transport (Uses HTTP) * Action: Allow the connection  1. On the **Action** menu, click **New Rule**. 2. Create a new outbound rule using the values in the following information.  * Rule Type: Predefined: Peer Distribution – Hosted Cache (Uses HTTP) * Action: Allow the connection |
| **Close the Group Policy Management Editor console** | 1. Close Group Policy Management Editor |
| **Close the Group Policy Management console** | 1. Close Group Policy Management. |

##### Verify Performance of HTTP Content Caching

Perform the steps in the following table while logged on as a member of the Enterprise Admins security group.

**Note:** Perform these steps on two client computers that have the Group Policy configuration settings and is on the other side of a WAN connection from the server.

Table 16: Verify Performance of HTTP Content Caching

|  |  |
| --- | --- |
| **High-level task** | **Details** |
| **Start Internet Explorer on the first client computer** | 1. On the first client computer, on the Quick Launch bar, click **Internet Explorer.** |
| **Download the HTTP content on the first client computer** | 1. In Internet Explorer, go to http\_site (where http\_site is the URL to the web site where the content is located). 2. Save content from the site (such as a file or graphic) 3. Record the download speed of the content while waiting for the content to download. |
| **Start Internet Explorer on the second client computer** | 1. On the second client computer, on the Quick Launch bar, click **Internet Explorer.** |
| **Download the HTTP content on the second client computer** | 1. In Internet Explorer, go to http\_site (where http\_site is the URL to the web site where the content is located). 2. Save content from the site (such as a file or graphic) 3. Record the download speed of the content while waiting for the content to download.   **Note:** The content should download almost immediately because the content is being downloaded from the hosted cache. |
| **Review the size of the hosted cache** | 1. On the server with BranchCache feature enabled, at a command prompt, type the following command and then press **Enter**.   Netsh peerdist show status all  The value of Current Cache Size indicates how much data is stored in the hosted cache. |

#### Hosted Caching for SMB Content: Step-by-step Feature Review

To review how the Hosted Caching feature works for SMB content, you need to complete the following tasks:

1. Create a BranchCache-enabled shared network folder
2. Publish files hashes and generate file hashes for files stored in the network shared folder.
3. Verify the performance of SMB content caching

**Note:** Perform these steps in a test environment as these steps could adversely affect your production environment. Also, you need to have a method of simulating a WAN connection to perform these steps.

##### Create a BranchCache-enabled Shared Network Folder

Perform the steps in the following table while logged on as a member of the Enterprise Admins security group.

Table 17: Configure BranchCache Feature for HTTP Content Caching

|  |  |
| --- | --- |
| **High-level task** | **Details** |
| **Start Server Manager** | 1. On the Start menu, point to **Administrative Tools**, and then click **Share and Storage Management**. |
| **Create a BranchCache-enabled shared network folder** | 1. In the Share and Storage Management, console in the **Actions** pane, click **Provision Share**. 2. In **Location**, type **C:\inetpub\wwwroot**, and then click **Next**. 3. On the **Permissions** page, click Next 4. In **Share name**, type **CorpFiles**, and then click **Next**. 5. Click **Advanced**. 6. On the **Caching** tab, click **Enable Windows Branch Cache**, and then click **OK**. 7. On the **SMB Settings** page, click **Next**. 8. On the **SMB Permissions** page, click **Next**. 9. On the **DFS Namespace Publishing** page, click **Next**. 10. Click **Create**. 11. Click **Close**. |

##### Publish File Hashes and Generate File Hashes

Perform the steps in the following table while logged on as a member of the Enterprise Admins security group.

Table 18: Publish File Hashes and Generate File Hashes

|  |  |
| --- | --- |
| **High-level task** | **Details** |
| **Start Server Manager** | 1. On the Start menu, in **Start Search**, type **gpedit.msc**, and then press **Enter**.   The Local Group Policy Editor starts. |
| **Configure the Hash Publication settings** | 1. In the Local Group Policy Editor console, go to **Computer Configuration/Administrative Templates/Network/LanManServer**. 2. Change the value of **Hash Publication for Windows Branch Cache** to **Enabled**, and verify that **Allow has publication for all shares** is selected. 3. Close the Local Group Policy Editor console. |
| **Generate file hashes** | 1. At a command prompt, type the following command and then press **Enter** (where server\_name is the name of the server you configured)   Hashgen –s [\\server\_name\corpfiles](file:///\\server_name\corpfiles) |

##### Verify the Performance of SMB Content Caching

Perform the steps in the following table while logged on as a member of the Enterprise Admins security group.

Table 19: Verify the Performance of SMB Content Caching

|  |  |
| --- | --- |
| **High-level task** | **Details** |
| **Access shared network folder on the first computer** | 1. On the first client computer, on the Start menu, in **Start Search**, type **\\**server\_name**\corpfiles**, and then press **Enter** (where server\_name is the name of your server where BranchCache is enabled). |
| **Download the SMB content on the first client computer** | 1. Copy a file from the shared network folder. 2. Record the download speed of the content while waiting for the content to download. |
| **Access shared network folder on the second computer** | 1. On the second client computer, on the Start menu, in **Start Search**, type **\\**server\_name**\corpfiles**, and then press **Enter** (where server\_name is the name of your server where BranchCache is enabled). |
| **Download the SMB content on the second client computer** | 1. Copy the same file from the shared network folder. 2. Record the download speed of the content while waiting for the content to download.   **Note:** The content should download almost immediately because the content is being downloaded from the hosted cache. |

### Improved Security for Branch Offices

Windows Server 2008 introduced the read-only domain controller feature, which allows a read-only copy of Active Directory® Domain Services (AD DS) to be placed in less secure environments such as branch offices. Windows Server 2008 R2 introduces support for read-only copies of information stored in Distributed File System (DFS) replicas, as illustrated in the following figure.

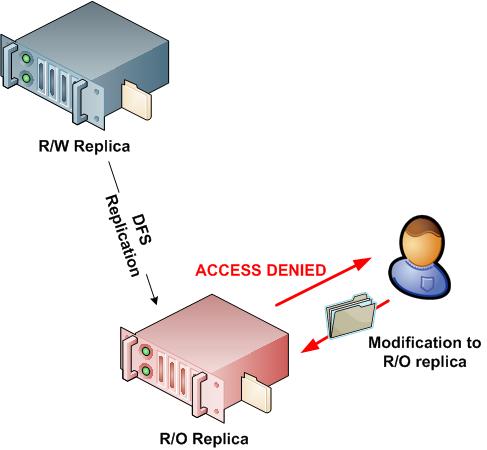


Figure 31: Read-only DFS in a branch office scenario

Read-only DFS replicas helps protect your digital assets by allowing branch offices read-only access to information that you replicate to the offices by using DFS. Because the information is read-only, users are unable to modify the content stored in read-only DFS replicated content and thereby protects data in DFS replicas from accidental deletion at branch office locations.

### More Efficient 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 advantage 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.

### Improved Virtualized Desktop Integration

Windows 7 introduces the RemoteApp & Desktop (RAD) feeds 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. For a detailed description of RDS and VDI, see the “Terminal Services Becomes Remote Desktop Services for Improved Presentation Virtualization” section earlier in this guide.

### Higher Fault Tolerance for Connectivity Between Sites

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 problem with existing VPN solutions is that 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 reestablished, resulting in momentary connectivity outages.

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, with no interruption of connectivity.

### Increased Protection for Removable Drives

In Windows Server 2008 and prior operating systems primarily used BitLocker Drive Encryption (BitLocker) 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 drives, or CompactFlash 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.

BitLocker keys can also be archived in AD DS, which provide an extra level of protection in the event that 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.

### Improved 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, when 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 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.