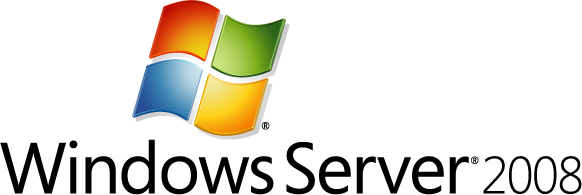
****

Windows Server 2008 Condensed Technical Overview

Published: January 2008

© 2008 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, PowerShell, SharePoint, SoftGrid, Windows, Windows Media, 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.

Table of Contents

[Introduction 5](#_Toc185320513)

[Overview 5](#_Toc185320514)

[Web and Applications 5](#_Toc185320515)

[Virtualization 5](#_Toc185320516)

[Security and Compliance 6](#_Toc185320517)

[Solid Foundation for Business Workloads 6](#_Toc185320518)

[Virtualization 7](#_Toc185320519)

[Server Virtualization with Hyper-V 7](#_Toc185320520)

[Security 7](#_Toc185320521)

[Strong Isolation 7](#_Toc185320522)

[Performance 8](#_Toc185320523)

[Simplified Management 8](#_Toc185320524)

[Presentation Virtualization 9](#_Toc185320525)

[Terminal Services RemoteApp 9](#_Toc185320526)

[Terminal Services Web Access 10](#_Toc185320527)

[Terminal Services Gateway (TS Gateway) 10](#_Toc185320528)

[Single sign-on 11](#_Toc185320529)

[Summary 11](#_Toc185320530)

[Web & Applications 11](#_Toc185320531)

[Introduction 11](#_Toc185320532)

[Internet Information Services 7.0 (IIS 7.0) 12](#_Toc185320533)

[Improved management tools 12](#_Toc185320534)

[Modular feature-based installation 12](#_Toc185320535)

[Distributed Configuration Model 12](#_Toc185320536)

[Diagnostics & Troubleshooting 13](#_Toc185320537)

[Strong Web Application Support 13](#_Toc185320538)

[Extensible modular architecture 14](#_Toc185320539)

[Flexible extensibility model for customization 14](#_Toc185320540)

[True application XCopy deployment 14](#_Toc185320541)

[Windows Media Services 14](#_Toc185320542)

[Summary 15](#_Toc185320543)

[Server Management 15](#_Toc185320544)

[Introduction 15](#_Toc185320545)

[Initial Configuration Tasks 16](#_Toc185320546)

[Server Manager Console 16](#_Toc185320547)

[Server Manager Wizards 16](#_Toc185320548)

[Group Policy Preferences 16](#_Toc185320549)

[Windows PowerShell 17](#_Toc185320550)

[Windows Remote Management 18](#_Toc185320551)

[Server Core 18](#_Toc185320552)

[Windows Server 2008 Print Management 19](#_Toc185320553)

[Windows Deployment Services 19](#_Toc185320554)

[Security & Compliance 20](#_Toc185320555)

[Introduction 20](#_Toc185320556)

[Identity and Access in Windows Server 2008 21](#_Toc185320557)

[Network Access Protection 22](#_Toc185320558)

[Windows Firewall Advanced Security Functionality 22](#_Toc185320559)

[BitLocker Drive Encryption 23](#_Toc185320560)

[Active Directory Federation Services 23](#_Toc185320561)

[Service-based AD DS 23](#_Toc185320562)

[Enterprise PKI (PKIView) 24](#_Toc185320563)

[V3 Certificate Templates 24](#_Toc185320564)

[Federated Rights Management in Windows Server 2008 25](#_Toc185320565)

[Cryptography Next Generation (CNG) 25](#_Toc185320566)

[Read-Only Domain Controllers 26](#_Toc185320567)

[Server and Domain Isolation 26](#_Toc185320568)

[Remote Locations 27](#_Toc185320569)

[Introduction 27](#_Toc185320570)

[Deployment and Administration 27](#_Toc185320571)

[Read-Only Domain Controllers 28](#_Toc185320572)

[BitLocker Drive Encryption 28](#_Toc185320573)

[Server Core 28](#_Toc185320574)

[Enhanced Manageability of Active Directory 28](#_Toc185320575)

[High Availability 29](#_Toc185320576)

[Introduction 29](#_Toc185320577)

[Failover Clustering 29](#_Toc185320578)

[Clustering and Hyper-V 30](#_Toc185320579)

[Network Load Balancing 31](#_Toc185320580)

[Windows Backup 32](#_Toc185320581)

[Summary 32](#_Toc185320582)

# Introduction

## Overview

Microsoft® Windows Server® 2008, with built-in Web and virtualization technologies, is designed to provide organizations with increased reliability and flexibility for their server infrastructure. New virtualization tools, Web technologies, and security enhancements save time, reduce costs, and provide a platform for a dynamic datacenter. Powerful new tools, such as Internet Information Services 7.0 (IIS 7.0), Windows Server Manager, and Windows PowerShell, offer more control over servers and streamline Web, configuration, and management tasks. Advanced security and reliability enhancements like Network Access Protection (NAP) and the Read-Only Domain Controller (RODC) harden the operating system and protect the server environment to help create a solid foundation on which to build businesses.

## Web and Applications

Windows Server 2008 is a powerful Web Application and Services Platform that helps organizations to deliver rich Web-based experiences efficiently and effectively. The release of Internet Information Services 7.0 (IIS 7.0) as part of Windows Server 2008 offers improved administration and diagnostics, better development and deployment tools, and lower infrastructure costs. IIS 7.0 is also a completely modular, extensible Web server with expanded application hosting, while retaining excellent compatibility and solving important customer challenges. The IIS 7.0 architecture delivers highly available, secure, and scalable Web-based applications and services. IIS 7.0 offers robust application support for classic ASP, ASP.NET, XML, and PHP, providing organizations with the flexibility to write applications in the language that they prefer, and to host applications on the platform that best meets their needs.

Microsoft Windows Media® Services is an industrial-strength platform for streaming live or on-demand audio and video content over the Internet or an intranet. Windows Media Services provide the ultimate fast-streaming experience and dynamic programming for on-the-fly and personalized content delivery, on a platform that offers ease-of-administration, customization, and scalability.

## Virtualization

With its built-in server virtualization technology, Windows Server 2008 enables organizations to reduce costs, increase hardware utilization, optimize their infrastructure, and improve server availability. Windows Server Hyper-V™ uses a 64-bit hypervisor-based platform for increased reliability and scalability. Hyper-V helps organizations optimize their hardware resources through server consolidation. Hyper-V also leverages components of the Windows Server 2008 platform, like failover clustering to provide high availability, and Network Access Protection (NAP) to quarantine non-compliant virtual machines.

Another form of virtualization is Presentation Virtualization, which is the ability to detach the application presentation layer, or the user interface, from the host operating system. In Windows Server 2008, Terminal Services Gateway and Terminal Services RemoteApp™ provide centralized application access with integration of remote applications on client computers, and easy access to these same remote programs using a Web browser. Terminal Services also provide a means to access remote terminals and applications across firewalls. (For detailed information about Terminal Services, see the section covering Centralized Application Access.)

## Security and Compliance

Windows Server 2008 is the most secure Windows Server ever. Its hardened operating system and security innovations, including Network Access Protection, Federated Rights Management, and Read-Only Domain Controller, provide unprecedented levels of protection for an organization’s data. Windows Server 2008 includes security and compliance enhancements, more advanced encryption, and tools that improve auditing and secure startup. It helps organizations to prevent data theft with Rights Management Services and Windows BitLocker™ Drive Encryption.

Windows Service Hardening helps keep systems safer by preventing critical server services from being compromised by abnormal activity in the file system, registry, or network. Security is also enhanced in the Windows Server 2008 operating system by means of Network Access Protection (NAP), Read-Only Domain Controller (RODC), Public Key Infrastructure (PKI) enhancements, a new Windows Firewall with improved filtering, and next-generation cryptography support.

Windows Server 2008 delivers a fully-integrated Federated Rights Management Services solution. This allows organizations to easily extend their Rights Management framework, allowing critical information to be securely shared with partners without the overhead of maintaining additional user accounts for users outside the organization.

## Solid Foundation for Business Workloads

Windows Server 2008 is the most flexible and robust Windows Server operating system to date. With new technologies and features such as the Server Core installation option, Windows PowerShell, Windows Deployment Services, and enhanced networking and clustering technologies, Windows Server 2008 provides the most versatile and reliable Windows-based platform for all workload and application requirements.

Server Manger integrates server role and feature addition, removal, and configuration into a single Microsoft Management Console (MMC). Windows Deployment Services (WDS) is a suite of components that work together on Windows Server 2008 to provide a simplified, secure, and rapid Windows operating system deployment to clients and servers. WDS uses network-based installation, without the need for an administrator to work directly on each computer, or to install Windows components from CD or DVD media. The Windows PowerShell command-line shell and scripting language helps IT Professionals to automate common tasks, and to control system administration more easily. It also accelerates automation, even in remote locations, such as branch offices. PowerShell leverages existing investments by retaining compatibility with existing scripting solutions.

Server Core is a new installation option for selected server roles that includes only the necessary subsystems required for those roles. Server core can create a more reliable and secure server that requires less patching and servicing.

Windows Server 2008 includes the enhanced and improved TCP/IP stack. This next generation TCP/IP stack improves security by providing filtering capabilities at all layers of the TCP/IP stack. It also provides improved future-proof security at the platform level while ensuring backward compatibility.

A failover cluster—formerly known as server clusters—is a group of independent computers that work together to increase the availability of applications and services. In Windows Server 2008, the improvements to failover clusters simplify administration, make them easier to secure, and more stable.

# Virtualization

## Server Virtualization with Hyper-V

Windows Server 2008 includes Hyper-V, a powerful virtualization technology with strong management and security features. Hyper-V enables businesses to leverage their existing familiarity with Windows Server management and take advantage of virtualization's flexibility and security benefits without buying third-party software. Microsoft and its partners provide comprehensive support for Windows and supported Linux guest operating systems. Hyper-V is a highly flexible, high-performance, cost-effective, well-supported virtualization platform.

## Security

Security is a core challenge in every server implementation. A server hosting multiple virtual machines (VMs)—also known as consolidated servers—is exposed to the same security risks as non-consolidated servers, but adds the challenge of administrator role separation. Hyper-V helps increase security for consolidated servers and addresses the challenge of administrator role separation. Hyper-V accomplishes this through the following features:

* Strong partitioning ‑ A virtual machine functions as an independent operating system container that is completely isolated from other virtual machines running on the same physical server.
* Hardware-level security‑ Features such as Data Execute Prevention (DEP) are available in newer server hardware, which helps prevent execution of the most prevalent viruses and worms.
* Role-based security ‑ Hyper-V helps prevent exposure of VMs that contain sensitive information, and also protects the underlying host operating system from compromise by a guest operating system.
* Network security features ‑ These features enable automatic Network Address Translation (NAT), firewall, and Network Access Protection (NAP).
* Minimal Trusted Computing Base ‑ This gives a reduced attack surface and streamlined, lightweight virtualization architecture. This feature enhances the reliability of Virtual Machines based on Hyper-V.

Configuring a consolidated server that provides the best security and operating system environment for every application can present a difficult challenge in some cases. Because Hyper-V creates an environment where it is possible to configure each workload with an ideal operating system environment and security profile, Hyper-V addresses the challenge of role separation on a consolidated server. Hyper-V protects VMs and the host operating system from each other by allowing VMs to run under a service account with only needed privileges. With Hyper-V, the host operating system is protected and a compromised VM is limited in the damage it could cause to other VMs.

## Strong Isolation

Server virtualization enables workloads with varying resource requirements to coexist on the same host server. Hyper-V offers several features that facilitate effective usage of the host server’s physical resources:

* Flexible virtual machine configuration ‑ Virtual machines can be assigned guaranteed amounts of memory and multiple processors (with Windows Server 2008 guests). This feature allows administrators to create a Hyper-V configuration that balances individual VM resource needs against overall performance.
* Flexible networking configuration ‑ Hyper-V provides advanced network features for VMs, including NAT, firewall, and VLAN assignment. This flexibility can be used to create a Hyper-V configuration that better supports network security requirements.

The flexible memory assignment and flexible networking configuration features of Hyper-V provide a more effective response to dynamic server loads.

## Performance

Design advances and integration with virtualization-aware hardware enable Hyper-V to virtualize much more demanding workloads than previous versions, and with greater flexibility in resource assignment.

Performance advancements include:

* Lightweight, low-overhead virtualization architecture based on a 64-bit Hypervisor. Virtualization-aware hardware—Intel VT and AMD “Pacifica” technology—enables higher guest operating system performance.
* Multi-core support. Windows Server 2008 guests can be assigned up to four logical processors. This enables virtualizing large, compute-intensive workloads that benefit from the parallel processing benefits of a multi-processor VM cores.
* 64-bit host and guest operating system support. Hyper-V runs on the 64-bit version of Windows Server 2008 to provide access to large pools of memory for guest VMs. Memory-intensive workloads that would suffer from extensive paging when executed on a 32-bit operating system can be successfully virtualized under Hyper-V. Hyper-V also supports 64-bit and 32-bit guest operating systems running on the same consolidated server.
* Server Core support. Hyper-V can use a Server Core installation of Windows Server 2008 as a host operating system. The minimal install footprint and low overhead of Server Core dedicate the greatest possible amount of host server processing capability to running VMs. In addition, the reduced patching requirements for Server Core will minimize the number of reboots required for Hyper-V.
* Pass-through disk access. Guest operating systems can be configured to directly access local or iSCSI Storage Area Network (SAN) storage, providing higher performance for I/O-intensive applications, such as SQL Server® or Microsoft Exchange.

Many server workloads place heavy demands on server processing and I/O subsystems. Applications like SQL Server and Microsoft Exchange are traditionally heavy users of memory and disk throughput, and there has been reluctance to virtualize these workloads. The 64-bit Hypervisor in Hyper-V along with features like pass-through disk access make it possible and often desirable to virtualize large workloads.

## Simplified Management

In the datacenters and remote branch office installations where Hyper-V may be deployed, strong management and automation capabilities are required to fully realize the cost reducing potential of virtualization. Hyper-V meets this challenge with the following management and automation capabilities:

* Extensible management ‑ Hyper-V is designed to work with Microsoft System Center Operations Manager (SCOM) and System Center Virtual Machine Manager (SCVMM). These management tools provide reporting, automation, deployment, and user self-service tools for Hyper-V.
* MMC 3.0 interface for VM management ‑ The familiar Microsoft Management Console interface is used to manage Hyper-V configuration and VM settings, reducing the Hyper-V learning curve significantly.
* Windows Management Instrumentation (WMI) interface ‑ Hyper-V incorporates a WMI provider that provides system information and scriptable management access.
* Windows PowerShell scripting ‑ Hyper-V host and VM configuration is configurable through Windows PowerShell.
* Windows Hyper-V ‑ This version of Windows provides organizations that intend to virtualize with a low cost option for deploying Hyper-V. This standalone version of the Hyper-V hypervisor is suitable for lights-out and remote management scenarios like datacenters and remote infrastructures.

The management capabilities of SCOM and SCVMM make it possible to effectively manage both datacenter installations and highly distributed installations of Hyper-V. For example, script access to the WMI provider in Hyper-V could be used to automate maintenance windows on multiple Hyper-V host servers by powering down guest VMs, powering them up on a standby server, performing host server maintenance, and then restoring the VMs to their original host. With the addition of System Center Virtual Machine Manager, this operation can be automated and performed with no perceptible downtime for many applications.

## Presentation Virtualization

Presentation virtualization is another key component of the Windows Server 2008 virtualization solution. Terminal Services (TS) presentation virtualization, which separates where an application is used from where it is run, enables clients to run any application. TS presentation virtualization accelerates and extends application deployment to a wide variety of client devices, making an organization’s IT infrastructure more agile and responsive.

Applications deployed with Terminal Services are installed only once in the datacenter, and not locally on client computers. This simplifies both the delivery and the ongoing maintenance of applications. New applications can be deployed to a wide variety of clients with Terminal Services, including clients that cannot run the new application natively. Microsoft Application Virtualization for Terminal Services virtualizes applications on the Terminal Server, isolating them from each other. This increases server utilization with more applications and users on each Terminal Services server.

Terminal Services presentation virtualization simplifies remote connectivity. It improves remote worker efficiency by enabling rich applications to be accessed from a Web page and seamlessly integrated with a local desktop.

## Terminal Services RemoteApp

Terminal Services presentation virtualization helps organizations keep critical intellectual property secure. It also simplifies regulatory compliance by removing applications and data from the desktop. With TS applications and data live in the datacenter, and only encrypted keyboard and mouse strokes are transmitted over the network.

With Terminal Services RemoteApp™, centralized applications appear to be local applications. The remote application launches, not the entire remote desktop; it runs in its own resizable window on the desktop of the client computer. If the program uses a notification area icon, that icon appears in the client’s notification area. Pop-up windows are redirected to the local desktop and local drives and printers are redirected and made available within the remote program. Users may be unaware that the remote program is different than other local applications running side-by-side with the remote program on their desktop.

Other RemoteApp improvements are:

* Remote Desktop Connection 6.1 ‑ To access Terminal Services, users will need to use the Remote Desktop Connection 6.1. It is included with both Windows Server 2008 and Windows Vista®, and is available as free a download for Windows® XP and Windows Server® 2003.
* Remote Desktop Connection Display Improvements ‑The Remote Desktop Connection 6.1 software adds support for higher-resolution desktops (up to 4096 x 2048) and spanning multiple monitors horizontally to form a single large desktop. Remote Desktop Connection 6.1 users can take advantage of newer high resolution monitors and modern display formats, like 16:9 or 16:10 widescreen formats, that do not conform to the previous 4:3 standard.
* Desktop Experience ‑Remote Desktop Connection 6.1 reproduces on the user’s client computer the desktop that exists on the remote computer. With Desktop Experience installed on Windows Server 2008, the user can access Windows Vista features, such as Windows Media® Player, desktop themes, and photo management within his or her remote connection. The desktop experience feature and the display data prioritization settings—designed to keep the keyboard and mouse in sync with what displays on the monitor even under heavy bandwidth usage—enhance the end-user experience when connecting to a Windows Server 2008 Terminal Server.

RemoteApp reduces administrative effort by having only one central application on the server to maintain, instead of having to maintain individual installations on multiple desktop computers throughout the organization. It also improves the user experience, providing smoother integration of the remote application with the client computer desktop.

## Terminal Services Web Access

Terminal Services Web Access (TS Web Access) instantly Web-enables native Windows applications without costly re-coding, and allows users to access the applications from a secure Web page. TS Web Access quickly and easily connects remote workers with the critical applications they need to be productive.

TS Web Access lets administrators make Terminal Services RemoteApp programs available to users from a Web browser without requiring the user to install any software. With TS Web Access, users can visit a Web site and access a list of all available applications. When the user starts one of the listed programs, a Terminal Services session is automatically started for that user on the Windows Server 2008-based Terminal Server hosting that application. For the user, this Web interface provides him or her a centralized menu that shows all remote applications that are currently available; running a remote application is as simple as choosing a program from the menu.

By using TS Web Access, administrative overhead is reduced. Programs can be easily accessed from a central location. Because programs are running on a terminal server and not on the client computer, the IT staff has a single instance of the application to maintain and update.

## Terminal Services Gateway (TS Gateway)

Terminal Services Gateway (TS Gateway) securely connects internal applications and data to mobile workers located outside the organization’s firewall. TS Gateway enables organizations to make selected servers and workstations easily and securely available to remote or traveling workers without their having to use a VPN connection. Some of the benefits of TS Gateway are:

* Leverages the security and availability of the HTTPS protocol to deliver Terminal Services with no client configuration.
* Provides a comprehensive security configuration model that enables administrators to control access to specific resources on the network.
* Enables users to connect remotely to terminal servers and remote workstations across firewalls and network address translators (NATs).
* Provides a more secure model, allowing users to access only selected servers and workstations, instead of the entire corporate network through a VPN.

Terminal Services Gateway provides a secure and easy way for organizations to provide remote users with access to servers and workstations within the network without having to install and configure a VPN connection. The comprehensive security features also enable the administrators to control access to specific resources.

## Single sign-on

Single sign-on allows users with a domain account to log on to a Terminal Services session one time, using a password or a smart card, and then gains access to remote servers and applications without being prompted for their credentials again. Single sign-on improves the user experience by eliminating the need for users to enter credentials every time they initiate a remote session.

## Summary

Microsoft Windows Server virtualization combines features that address many of the most difficult virtualization challenges, including: securing consolidated servers, responding to dynamic workloads, achieving high performance for virtualized workloads, and simplified management. The combination of security and strong VM isolation features in Hyper-V make it possible to consolidate heterogeneous workloads on Hyper-V host servers while maintaining flexibility and security. The 64-bit Hypervisor architecture that forms the foundation for Hyper-V provides high performance for demanding workloads. And the strong, integrated management features in Windows Server 2008, System Center Operations Manager and System Center Virtual Machine Manager, allow automated and effective control in a wide variety of virtualized environments.

Presentation virtualization with RemoteApp in Windows Server 2008 enables users to run remote applications on their own desktop, side by side with local applications. It also provides new options for accessing available applications through Terminal Services Web Access, giving users easier access to RemoteApp applications using a Web browser.

# Web & Applications

## Introduction

Windows Server 2008 provides a secure, easy-to-manage platform for developing and reliably hosting applications and services that are delivered from the server or over the Web. New features include simplified management, increased security, and both performance and extensibility improvements. In addition, enterprises will enjoy more efficient application and services management, quicker deployment and configuration of Web application and services, and a more secure, streamlined, customized Web platform. Windows Server 2008 provides Web applications and services greater performance and scalability, while allowing administrators fine control and visibility into how and when applications and services utilize vital operating system resources. Windows Server 2008 also includes best-of-breed collaboration technology designed to improve business processes, enhance team productivity, and provide a flexible platform for creating Web-based, collaborative applications. It also provides an industrial-strength platform for streaming live or on-demand audio and video content over the Internet or an intranet.

## Internet Information Services 7.0 (IIS 7.0)

Windows Server 2008 delivers a unified platform for Web publishing that integrates Internet Information Services 7.0 (IIS 7.0), ASP.NET, Windows Communication Foundation, and Windows SharePoint® Services. IIS 7.0 is a major advancement to the existing IIS Web server, and plays a central role in integrating Web platform technologies. Important benefits of IIS 7.0 include more efficient administration and management features, improved security, and reduced support costs. These features help create a unified platform that delivers a single, consistent development, and an administrative model for Web solutions.

## Improved management tools

The new administration utility in IIS 7.0, IIS Manager, is a more efficient tool for managing the Web server. It provides support for IIS and ASP.NET configuration settings, user data, and runtime diagnostic information. The new user interface (UI) also enables those who host or administer Web sites to delegate administrative control to developers or content owners, thus reducing cost of ownership and administrative burden for the administrator. The new IIS Manager interface supports remote administration over HTTP, allowing for integrated local, remote, even cross-Internet administration, without requiring DCOM or other administrative ports be opened on the firewall.

A new command-line tool, appcmd.exe, is also included for managing and administering Web servers, Web sites and Web applications. The command-line interface simplifies common management Web server tasks for administrators. For example, appcmd.exe could be used to list Web server requests that have been forced to wait for more than 500 milliseconds. This information could be used to troubleshoot applications that are performing poorly. The output of appcmd.exe can be piped into other commands for further processing.

## Modular feature-based installation

IIS 7.0 is made up of more than 40 separate feature modules. Only half of the modules are installed by default, and administrators can selectively install or remove any feature modules they choose. This modular approach allows administrators to install only the options they need, and saves time by limiting the number of features that must be managed and updated. In addition, because no unnecessary software is running, the attack surface of the Web server is reduced, improving security.

## Distributed Configuration Model

IIS 7.0 introduces major improvements to the way its configuration data is stored and accessed. One of the important goals of the IIS 7.0 release is to enable distributed configuration of the IIS settings, allowing administrators to specify IIS configuration settings in files that are stored with the code and content.

Distributed configuration enables administrators to specify configuration settings for a Web site or application in the same directory where the code or content is stored. By specifying configuration settings in a single file, distributed configuration allows administrators to delegate administration of selected Web site features or Web applications to others. For example, a Web site might be delegated so that the application developer can configure the default document used for that Web site. Administrators can also lock specific configuration settings so that they cannot be changed by anyone else. This feature might be used to ensure that a security policy, which prevents script execution, is not overridden by a content developer who has been delegated administrative access to the Web site. By using distributed configuration, the configuration settings for a specific site or application can be copied from one computer to another as the application moves from development into test, and ultimately into production.

## Diagnostics & Troubleshooting

IIS 7.0 helps make troubleshooting the Web server easier than ever with built-in diagnostics and tracing support, allowing the administrator to peer into the Web server and see detailed, real-time diagnostic information. Diagnostics and troubleshooting allow a developer or an administrator to see requests that are running on the server. IIS 7.0 also includes new Runtime Status and Control objects, which provide real-time state information about application pools, worker processes, sites, application domains, and even running requests. This information can be used to determine, for example, which request in a worker process is consuming 100% of the CPU.

IIS 7.0 also includes detailed trace events throughout the request and response path, allowing developers and administrators to trace a request as it makes its way through the IIS request processing pipeline, into any existing page level code, and then back to the response. These detailed trace events allow developers to understand not only the request path and any error information that was raised as a result of the request, but also elapsed time and other debugging information to assist in troubleshooting all types of errors.

IIS 7.0 also simplifies troubleshooting by providing error messages that are much more detailed and actionable. The new custom errors module in IIS 7.0 allows for detailed error information to be sent back to the browser (by default, to localhost), and configurable to be sent to other remote clients. Instead of seeing a terse error code, administrators now can see detailed information about the request, what potential issues may have caused the error, and also suggestions about how to fix it.

One of the most important features which helps improve IIS 7.0 troubleshooting support is the Runtime Status and Control API (RSCA), which is designed to give detailed runtime information about the server from deep within IIS 7.0. With RSCA, it is possible to inspect and manage various entities including sites, application pools, and even .NET Framework application domains. RSCA also surfaces, in real time, currently executing requests on the server. RSCA data is available from the WMI provider and managed API (Microsoft.Web.Administration). The IIS 7.0 admin GUI and command-line tool also reveals this data for administrators.

## Strong Web Application Support

The cost of Web application development and deployment continues to increase because of the vast number of software technologies and hardware platforms with which applications must be compatible. Customers expect robust and full-featured Web applications and services that rely on a variety of languages- such as classic ASP, ASP.NET, and PHP. A Web hosting platform that supports all of these languages while offering powerful and easy-to-use management tools will enable organizations to run all of their Web applications on one platform. This can reduce or even eliminate the need to run multiple host platforms, and lower support costs. Web hosting platforms that do not support all of these languages in an integrated way can add to the cost of development and maintenance, result in lost business, and reduce the ability of their applications and services to adapt to changing business needs.

IIS 7.0 delivers a unified platform for Web hosting and publishing and provides application support that goes well beyond classic ASP. An important feature of IIS 7.0 is the FastCGI module. FastCGI is a high-performance version of the Common Gateway Interface (CGI), which is the standard Web interface that many Web client applications use to communicate with Web servers. FastCGI enables CGI-based Web applications to run faster while maintaining stability and providing reliable PHP support. This makes IIS 7.0 an excellent platform that organizations can use to host of all of their Web applications.

IIS 7.0 also operates with Microsoft .NET Framework version 3.0, which combines new technologies for building applications that deliver a visually compelling user experience, communication across technology boundaries, identity management, and support for a wide range of business processes. .NET Framework 3.0 reduces development complexity by providing a consistent and comprehensive development environment, enabling solutions that work with a wide variety of mobile devices, backend services, and applications. By supporting classic ASP, ASP.NET, XML and PHP, IIS 7.0 provides organizations with the flexibility to write applications in the language of their choice, and to host applications on the platform that they want.

## Extensible modular architecture

In previous versions of IIS, all functionality was built in by default, and there was no easy way to extend or replace any of that functionality. As stated earlier, in IIS 7.0, the core is divided into more than 40 separate feature modules. The core also includes a new Win32® API for building core server modules. Core server modules are new and more powerful replacements for Internet Server Application Programming Interface (ISAPI) filters and extensions. ISAPI filters and extensions are still supported in IIS 7.0. Because all IIS core server features were developed using the new IIS 7.0 Win32 Module API as discrete feature modules, users can add, remove, or even replace IIS feature modules.

## Flexible extensibility model for customization

IIS 7.0 enables developers to extend IIS to provide custom functionality in new, more powerful ways. This is in part due to the all-new core server application programming interface (API) set that allows feature modules to be developed in both native code (C/C++) and managed code (languages such as C#, and Visual Basic® 2005, that use the .NET Framework). In fact, much of the IIS 7.0 feature set for request and application processing has been implemented using these same APIs. IIS 7.0 also enables extensibility for configuration, scripting, event logging, and administration tool feature sets, providing software developers with a complete server platform on which to build Web server extensions.

## True application XCopy deployment

IIS 7.0 allows IIS configuration settings to be stored in web.config files, which makes it much easier to use XCopy to copy applications across multiple Web servers, and to avoid costly and error-prone replication, manual synchronization, and additional configuration tasks.

## Windows Media Services

Windows Media Services is an industrial-strength platform for streaming live or on-demand audio and video content over the Internet or an intranet. Windows Media Services can be configure and manage multiple servers running Windows Media Services to deliver content to clients.

Windows Media Services provides the ultimate fast-streaming experience, dynamic programming for personalized content delivery, and an industrial-strength platform that ensures ease-of-administration, customization, and scalability.

Fast Streaming capabilities in Windows Media Services effectively eliminate buffering time, and reduce the likelihood of playback interruptions due to network conditions. Features like Fast Start, Fast Cache, Fast Recovery, and Fast Reconnect provide an always-on viewing experience by streaming content with minimal buffering and down-time, even over high latency network connections, such as wireless and satellite.

Windows Media Services enables dynamic content programming, so that organizations can instantly update and personalize content to provide the most compelling user experience. These programming capabilities include:

* Automatically program and seamlessly update digital media content as needed.
* Make program changes during on-demand or live broadcasts, change the order of clips, insert an ad, insert a new clip, and more, without interruption to the viewer.
* Generate revenue with a wide variety of advertising types, including lead-in or interstitial ads, which can easily be integrated with third-party advertising servers. Advanced reporting ensures tracking of how and when ads are viewed.
* Make streaming content more relevant and useful to each user by automatically generating personalized playlists that are tailored to individual audience members.

With Windows Server 2008, administrators can now install the Windows Media Services functionality services required to perform the Streaming Media Services role on a Server Core installation of Windows Server 2008.

## Summary

The structural changes in IIS 7.0 combine to create a very flexible Web application system. The ability to access IIS configuration through both a GUI interface and the appcmd.exe command-line tool provides effective tools for both novice Web server administrators with basic skills, and more advanced administrators who manage multiple servers using scripting tools. The tracing and troubleshooting components of IIS provide detailed, usable information that helps administrators and application developers isolate troublesome pages and code. The modularized functionality and granular administration model of IIS 7.0 make it easy for server administrators to create exactly the server they need, and allow only the required level of access to site and content managers. With Windows Media Services, Windows Server 2008 also provides a solid platform for delivering streaming media content.

# Server Management

## Introduction

From streamlining new server configuration to automating repetitive management tasks, simplifying the day-to-day complexities of server administration is a theme in many of the enhancements included in Windows Server 2008. Centralized management tools, intuitive interfaces, and automation features enable IT Professionals to more easily manage network servers, services, and printers, in both the central network and in remote locations.

## Initial Configuration Tasks

With Windows Server 2008, the streamlined installation process isn’t interrupted by configuration tasks that require user intervention. Those tasks and dialog boxes now occur after the primary installation has completed, freeing the administrator from having to interact with the installation sequence.

The Initial Configuration Tasks window is a new feature in Windows Server 2008 that helps an administrator to provision and set up a new server. It includes tasks such as setting the Administrator password, changing the name of the Administrator account to improve the security of the server, joining the server to an existing domain, and enabling Windows Update and Windows Firewall.

## Server Manager Console

Windows Server 2008 eases the task of managing and securing multiple server roles in an organization with the new Server Manager Console. The Server Manager Console provides a single, unified interface for managing a server’s configuration and system information, displaying server status, identifying problems with server role configuration, and managing all roles installed on the server.

Server Manager is built on the Service Modeling Language (SML) platform, which is used to model complex IT services and systems in software, including structure, constraints, configuration, and best practices. Server Manager takes advantage of the model-based management infrastructure provided by the SML platform. The hierarchy pane of the Server Manager console contains expandable nodes that allow administrators to go directly to consoles for managing specific roles, troubleshooting tools, or finding backup and disaster recovery options.

Roles and features installed by using Server Manager are secure by default. Administrators don’t need to run the Security Configuration Wizard following role installation or removal unless they want to change the default settings. Server Manager consolidates a variety of management interfaces and tools into a unified management console, enabling administrators to complete common management tasks without having to navigate between multiple interfaces, tools, and dialog boxes.

## Server Manager Wizards

Wizards in Server Manager streamline server deployment tasks in an enterprise by cutting deployment time, compared with earlier Windows Server versions. Most common configuration tasks, such as configuring or removing roles, defining multiple roles, and role services can now be completed in a single session using Server Manager Wizards.

Windows Server 2008 performs dependency checks as the user progresses through Server Manager wizards, ensuring that all of the prerequisite role services needed by a selected role are installed, and none are removed that remaining roles or role services might still require .

## Group Policy Preferences

In many organizations, IT staff must map drives and printers for users. This requires the IT staff to write and debug the script, and then run the scripts through a Group Policy object (GPO). Many other settings may also be deployed by means of logon scripts. Scripts are often scattered, seldom documented, and can be time consuming to troubleshoot, support, and modify.

Windows Server 2008 includes the new Group Policy preferences built-in to the Group Policy Management Console (GPMC). Additionally, administrators can configure preferences by installing the Remote Server Administration Tools (RSAT) on a computer running Windows Vista Service Pack 1 (SP1). RSAT is currently in beta and is expected to release shortly after Windows Server 2008. RSAT includes the updated GPMC.

Group Policy Preferences are different from Group Policy settings, in several important ways. Group Policy settings are managed settings that are enforced. Users cannot change policy settings. Group Policy Preferences are unmanaged settings that users can change. By explicitly deploying preferences rather than accepting the default operating system settings, organizations create configurations that are more compatible with their IT environment and that are specifically tailored to the organization and how its people use their computers.

In contrast to the less IT-friendly methods for deploying preferences, Group Policy preferences supply a centralized system for deploying preferences. It simplifies deployment, reduces configuration errors, and lowers IT costs. Rather than using complicated logon scripts to deploy mapped drives, for example, administrators can simply create a Group Policy object and edit its Drive Maps preference item. Using Group Policy Preferences allows organizations to potentially reduce or eliminate logon scripts in their IT environment.

Benefits of Group Policy Preferences include:

* Improving IT productivity by providing more than 20 new extensions
* Reducing the need for logon scripts
* Limiting configuration errors through precision targeting and easy-to-use interfaces
* Enhancing end-user satisfaction
* Minimizing image maintenance by deploying generic images and using Group Policy Preferences to update them
* Reducing overall image count by deploying generic images and using targeted Group Policy Preference settings for groups of users and computers

## Windows PowerShell

Windows PowerShell command-line shell and scripting language helps IT Professionals automate common tasks. Using a new admin-focused scripting language, more than 120 standard command-line tools, and consistent syntax and utilities, Windows PowerShell allows IT Professionals to more easily control system administration and to accelerate automation. Windows PowerShell is easy to adopt and use, because it works with the existing IT infrastructure and existing script investments. It allows users to automate system administration of basic server management tasks as well as specific server roles, such as Terminal Server.

Windows PowerShell integrates the command-line shell and scripting language to allow administrators to more efficiently complete and automate bulk system administration tasks. Windows PowerShell improves upon the Windows Command Prompt and Windows Script Host (WSH) by providing command-line tools, called cmdlets, that have the exact same syntax as the scripting language. The command that is typed in the Windows PowerShell command prompt is the same command that would be used in a script for automating the task across multiple servers.

Windows PowerShell supports an organization’s existing scripts (for example, .vbs, .bat, .perl) so the organization does not need to migrate its scripts to adopt Windows PowerShell. Existing Windows-based command-line tools will run from the Windows PowerShell command-line. By providing consistency of syntax and naming conventions and integration of scripting language with the interactive shell, Windows PowerShell reduces the complexity and time required to automate system administration tasks.

## Windows Remote Management

With the growing number of remote servers in branch offices and other locations, IT Professionals need better options for effectively managing off-site servers. Windows Remote Management provides a low-bandwidth, scriptable way to easily manage servers in remote locations.

The Windows Remote Manager is the Microsoft implementation of WS-Management Protocol, a standard SOAP-based protocol that allows hardware and operating systems to interoperate. Administrators can use Windows Remote Management scripting objects, the Windows Remote Management command-line tool, or the Windows Remote Shell command-line tool to obtain management data (information, for example, about objects such as disks, network adapters, services, or processes) from local and remote computers. If the computer runs a Windows operating system version that includes Windows Remote Management, the management data is supplied by Windows Management Instrumentation (WMI).

Administrators can also use Windows Remote Shell (WinRS), a command line tool that enables administrators to remotely execute most Cmd.exe commands using the WS-Management protocol. WinRS is a good alternative to using Secure Shell (SSH) for performing remote administration tasks from the command line, and works over firewall friendly HTTPS. Using HTTPS for remote administration can reduce firewall configuration challenges in many cases.

## Server Core

Beginning with Windows Server 2008, administrators can choose to install a minimal installation of Windows Server with specific functionality and without any unneeded features. Server Core provides an environment for running one or more of the following server roles:

* Hyper-V
* IIS 7.0
* Dynamic Host Configuration Protocol (DHCP) server
* Domain Name System (DNS) server
* File server
* Active Directory® Domain Services (AD DS)
* Active Directory Lightweight Directory Services (AD LDS)
* Windows Media Services
* Print Server

Server Core offers the following benefits to organizations:

* Reduced software maintenance **‑** Because Server Core installs only what is required to have a manageable server running the supported server roles, the server requires less software maintenance. With a smaller Server Core installation, the number of updates and patches are reduced, saving both WAN bandwidth usage by servers and administration time by the IT staff.
* Reduced attack surface **‑** Because there are fewer files installed and running on the server, there are fewer attack vectors exposed to the network; therefore, there is less of an attack surface. Administrators can install just the specific services needed for a given server, keeping the exposure risk to an absolute minimum.
* Fewer restarts required and reduced disk space required ‑ A minimal Server Core installation has fewer installed components that will need to be updated or patched, and the number of required restarts will be reduced. A Server Core installation installs the minimal files needed to provide the required functionality, so less disk space will be used on the server. By choosing to use the Server Core installation option on a server, administrators can reduce the management and software update requirements for a server while also reducing security risks.

With the Server Core installation option in Windows Server 2008, administrators can reduce the ongoing maintenance requirements for servers, and simplify their management. By running a minimal Server Core installation limited to just the required functionality, the IT staff will only need to install patches and updates for that server that directly impact the installed files.

## Windows Server 2008 Print Management

The larger the organization is, the larger the number of printers within the network is, and more time is required by the IT staff to install and manage those printers; all of which translates to increased operating expenses. Windows Server 2008 includes Print Management, which is an MMC snap-in that enables administrators to manage, monitor, and troubleshoot all of the printers within the organization—even those in remote locations—from a single interface.

Print Management provides up-to-the-minute details about the status of all printers and print servers on the network from one console. Print Management can help find printers that have an error condition, and it can also send e-mail notifications, or run scripts when a printer or print server needs attention. On printer models that provide a Web interface, Print Management can access this additional data. This allows information, such as toner and paper levels, to be managed easily, even when printers are in remote locations. In addition, Print Management can automatically search for and install network printers on the local subnet of local print servers.

Print Management saves the print administrator a significant amount of time when installing printers on client computers and in managing and monitoring printers. Rather than having to install and configure printer connections on individual computers, Print Management can be used with Group Policy to automatically add printer connections to client computer’s Printers and Faxes folder. This is an effective and time-saving way of adding printers for a large number of users who require access to the same printer, such as users in the same department, or all users in a branch office location.

The automation options and centralized control interface provided included in Print Management for installing, sharing, and managing printers simplifies administration, and reduces the time required by the IT staff to deploy printers.

## Windows Deployment Services

Windows Deployment Services (WDS) is a suite of components that work together on Windows Server 2008 to provide a simplified, secure means of rapidly deploying Windows operating systems to computers by using network-based installation. WDS eliminates the need for an administrator to work directly on each computer, or install Windows components from CD or DVD media. It contains a number of new or enhanced features that will save IT staff time. The three components in WDS are organized into the following three categories:

* Server components ‑ These components include a Pre-Boot Execution Environment (PXE) server and Trivial File Transfer Protocol (TFTP) server for network booting a client to load and install an operating system. Also included is a shared folder and image repository that contains boot images, installation images, and files that are needed specifically for network boot.
* Client components ‑ These components include a graphical user interface that runs within the Windows Pre-Installation Environment (Windows PE) and communicates with the server components to select and install an operating system image.
* Management components ‑ These components are a set of tools that are used to manage the server, operating system images, and client computer accounts.

Windows Deployment Services includes the Windows Deployment Services MMC snap-in, which provides rich management of all Windows Deployment Services features. WDS also provides several enhancements to the RIS feature set specifically designed to facilitate easy deployments of Windows Vista and Windows Server 2008. With Windows Deployment Services, IT staff can:

* Use the Sysprep.exe and the Windows Deployment Services snap-in to create a "capture image" that can then be used to create a custom image
* Use the Windows Deployment Services Capture Wizard to create and add an image prepared with Sysprep.exe
* Use the Windows Deployment Services snap-in to associate unattended installation files with Windows images
* Associate one or more language packs with an image, eliminating the need for unique images for each language an organization supports
* Use the Windows Deployment Services snap-in to create a "discover image" for use with computers that do not support PXE boot

Note: The next version of Business Desktop Deployment (BDD) 2007 is Microsoft Deployment. It is the recommended process and toolset to automate desktop and server deployment. Microsoft Deployment provides detailed guidance and job aids for every organizational role involved with large-scale deployment projects. More information can be found at the following link:

<http://www.microsoft.com/downloads/details.aspx?familyid=3bd8561f-77ac-4400-a0c1-fe871c461a89&displaylang=en&tm>

# Security & Compliance

## Introduction

Windows Server 2008 is the most secure Windows server ever, with a hardened security platform that provides secure policy-based access to the network and ensures sensitive information is not compromised. It enables businesses to host the most mission critical applications and workloads.

Windows Server 2008 has many features that improve security and compliance. Some important enhancements include:

* Enforced client health ‑ Network Access Protection (NAP) enables administrators to configure and enforce health and security requirements before allowing clients access to the network
* Monitor certificate authorities ‑ Enterprise PKI improves the ability to monitor and troubleshoots multiple certification authorities (CAs)
* Identity and Access ‑ Platform technologies designed to help organizations manage user identities and associated access privileges
* Firewall enhancements ‑ The new Windows Firewall with Advanced Security provides many security enhancements
* Encrypt and protect data ‑ BitLocker Drive Encryption protects sensitive data by encrypting the disk drive
* Cryptographic tools ‑ Next Generation Cryptology provides a flexible cryptographic development platform
* Server and Domain Isolation ‑ Server and domain resources can be isolated to limit access to authenticated and authorized computers
* Read-Only Domain Controller (RODC) **‑** The RODC is new type of domain controller install option that can be installed in remote sites that may have lower levels of physical security
* Secure Federated Collaboration ‑ Active Directory Rights Management Services (AD RMS) enables a new way to protect sensitive information that is both more comprehensive and easier to secure
* Encrypting File System ‑ A crucial security feature, Encrypting File System is useful for user-level file and folder encryption. For network file and folder encryption, it enables administrators to store Encrypting File System keys on smart cards

These improvements help administrators increase the security level of their organization, and simplify the management and deployment of security-related configurations and settings.

## Identity and Access in Windows Server 2008

Managing user identities is a top priority for many businesses today. People need to access multiple systems and resources on the corporate network, using different types of devices. Because many of these systems don't communicate with each other, it's not uncommon to have multiple identities for the same person. As a result, managing these redundant identities is complex, wastes time, and increases security risks due to errors and poor user password management.

Microsoft Identity and Access (IDA) solutions are a set of platform technologies and products designed to help organizations manage user identities and associated access privileges. With a focus on security and ease of use, these solutions help businesses boost productivity, reduce IT costs, and eliminate the complexity of identity and access management. Microsoft Identity and Access solutions fall into five distinct areas:

* Identity Management ‑ Automates identity and access management
* Information Protection **‑** Safeguards confidential data, no matter where it goes
* Federated Identities ‑ Collaborates securely across organizational boundaries
* Directory Services ‑ Simplifies management of users and devices
* Strong Authentication **‑** Extends secure access beyond user names and passwords by incorporating the latest cryptography standards and certificate management innovations

Windows Server 2008 provides the comprehensive and integrated identity and access platform. The Microsoft IDA platform is built on Active Directory and provides familiar interfaces for IT Professionals, developers, and information workers to ensure that an entire organization can participate in safeguarding sensitive information while easily collaborating with others inside and outside of the organization. Integrated support on Windows environments can be extended to support heterogeneous environments with readily available partner solutions. These platform capabilities are grouped into the following three categories of services, with each featuring several essential components:

* Directory Services
  + Read-Only Domain Controller (RODC)
  + Active Directory Federation Services (AD FS)
  + Directory Service Auditing
  + Service-based Active Directory Domain Services (AD DS)
* Information Protection
  + Federated collaboration
  + BitLocker Drive Encryption
  + Federated Rights Management
* Strong Authentication
  + Cryptography API
  + V3 certificate templates
  + Public Key Infrastructure (PKI)

## Network Access Protection

Network Access Protection (NAP) prevents noncompliant computers from accessing and compromising an organization’s network. NAP is used to configure and enforce client health requirements and to update, or remediate, noncompliant client computers before they can connect to the corporate network. With NAP, administrators can configure health policies that define such things as software requirements, security update requirements, and required configuration settings for computers that connect to the organization’s network.

NAP enforces health requirements by assessing the health of client computers, and limiting network access when client computers are noncompliant. Both client and server-side components assist in the remediation of noncompliant client computers, so that those client computers can obtain unlimited network access. If a client computer is determined to be noncompliant, it can be denied access to the network, given limited access to the network, or patched immediately to bring it into compliance.

NAP enforcement methods support four network access technologies that work in conjunction with NAP to enforce health policies: Internet Protocol security (IPsec) enforcement, 802.1X enforcement, virtual private network (VPN) enforcement for Routing and Remote Access, and Dynamic Host Configuration Protocol (DHCP) enforcement.

## Windows Firewall Advanced Security Functionality

The Windows Firewall with Advanced Security in Windows Server 2008 is a stateful host-based firewall that allows or blocks network traffic according to its configuration and the applications that are currently running to provide protect the network from malicious users and programs. Windows Firewall with Advanced Security reduces conflicts and coordination overhead between technologies, and provides centralized filtering and connection security rules and policies.

One new feature is the ability to support firewall interception of both incoming and outgoing traffic. A network administrator, for example, can configure the new Windows Firewall with a set of exceptions to block all traffic sent to specific ports, such as well-known ports used by virus software, or to specific addresses containing either sensitive or undesirable content. This protects the computer from viruses that might spread through the network, and protects the network from viruses that may try to spread from a compromised system.

Because the number of configuration options for Windows Firewall has increased, a new MMC snap-in named Windows Firewall with Advanced Security is added to Windows Server 2008 to simplify administration. With the new snap-in, network administrators can remotely configure settings for Windows Firewall on client workstations and servers—something that was not possible in previous versions of Windows Server without a remote desktop connection—thereby simplifying remote configuration and management.

In previous versions of Windows Server, Windows Firewall and IPsec were configured separately. Because both a host-based firewall and IPsec in Windows can block or allow incoming traffic, it is possible to create overlapping or contradictory firewall exceptions and IPsec rules. The new Windows Firewall in Windows Server 2008 has combined the configuration of both network services using the same GUI and command-line commands. This integration of firewall and IPsec settings simplifies firewall and IPsec configuration and helps prevent policy overlap and contradictory settings.

## BitLocker Drive Encryption

BitLocker Drive Encryption is a new security feature in Windows Server 2008 that helps to protect servers, workstations, and mobile computers. It is also available in Windows Vista Enterprise and Windows Vista Ultimate editions for protecting client computers and mobile computers. BitLocker encrypts the contents of a disk drive. This prevents an intruder who runs a parallel operating system, or runs other software tools, from breaking the file and system protections, or from performing offline viewing of the files stored on the protected drive.

BitLocker enhances data protection by bringing together two major sub-functions: system volume encryption and integrity-checking for early-boot components. The entire system volume is encrypted, including the swap and hibernation files, which increases the security of the remote servers in the branch office location. BitLocker addresses the threats of data theft or exposure from a lost, stolen, or inappropriately decommissioned PC. BitLocker also helps organizations comply with government regulations, such as U.S. statues Sarbanes-Oxley and HIPAA, which require the maintenance of extremely high standards for security and data protection.

Active Directory Federation Services

Active Directory Federation Services (AD FS) is server role in Windows Server 2008 that provides a highly extensible and secure identity access solution that can operate across multiple platforms. AD FS provides browser-based clients, both inside and outside the network, access to protected, Internet-facing applications, even when user accounts and applications are located in different networks or organizations.

In a typical scenario, an application is located in one network and a user account is in another network. Users are required to enter secondary credentials when they attempt to access the application. However, with AD FS, secondary accounts are not necessary. Instead, trust relationships can be used to project a user's digital identity and access rights to trusted partners. In a federated environment, each organization continues to manage its own identities, but each organization can securely project and accept identities from other organizations.

By deploying federation servers in multiple organizations business-to-business transactions can be facilitated between trusted partner organizations. Organizations that own and manage resources that are accessible from the Internet can deploy AD FS federation servers and AD FS–enabled Web servers that manage access to the protected resources for trusted partners.

## Service-based AD DS

In Windows Server 2008, Active Directory Domain Services (AD DS) is service-based, meaning it may now be stopped and started using Microsoft Management Console (MMC) snap-ins or from the command line. A service-based AD DS simplifies management by reducing the time required to perform offline operations, such as an offline defragmentation or authoritative restore. It also improves the availability of other services that are running on a domain controller by keeping them active while performing AD DS maintenance. Any clients that are specifically bound to a stopped domain controller would simply contact another domain controller through discovery.

## Enterprise PKI (PKIView)

There are many enhancements to the Public Key Infrastructure (PKI) in the Windows Server 2008 and Windows Vista operating systems. There have been increases in manageability throughout all aspects of Windows PKI, the revocations services have been redesigned, and there is a decreased attack surface for enrolment. Active Directory Certificate Services (AD CS) provides an integrated infrastructure that enables the secure exchange of information. AD CS helps customize services for issuing and managing the certificates used in public key technologies.

PKI enhancements include:

* Enterprise PKI (PKIView) ‑ Originally part of the Microsoft Windows Server 2003 Resource Kit, PKIView was called the PKI Health tool. PKIView is now a Microsoft Management Console (MMC) snap-in for Windows Server 2008. It is used to analyze the health state of CAs, and to view details for certificate authority (CA) certificates published in AD CS.
* Online Certificate Status Protocol (OCSP) **‑** An Online responder based on the Online Certificate Status Protocol (OCSP) can be used to manage and distribute revocation status information in cases where the use of conventional CRLs is not an optimal solution. Online Responders can be configured on a single computer or in an Online Responder Array.
* Network Device Enrollment Service (NDES) **‑** In Windows Server 2008, the Network Device Enrollment Service (NDES) is the Microsoft implementation of the Simple Certificate Enrollment Protocol (SCEP), a communication protocol that makes it possible for software running on network devices, such as routers and switches that cannot otherwise be authenticated on the network, to enroll for x509 certificates from a certification authority (CA).
* Web Enrollment **‑** The new Web Enrollment control is more secure, easier to script, and easier to update than the previous version.
* Group Policy and PKI **‑** Certificate settings in Group Policy enable administrators to manage certificate settings from a central location for all of the computers in the domain.

## V3 Certificate Templates

Certificate templates provide a practical way to implement certificate enrollment in a managed Active Directory environment with Enterprise Certificate Authority. The CA administrator can define the blueprint for certificates that are enrolled from Enterprise CAs. With Windows Server 2008, more certificate templates and certificate template properties became available. The new certificate template types in Windows Server 2008 are called V3 templates.

V3 templates can leverage the latest cryptographic algorithms introduced in Windows Server 2008. With V3 certificate templates, administrators can also ensure that CA related communications between clients and the CA occur in the most secure fashion. Windows Server 2008 also introduces a completely new default template that allows clients to validate the certificate source using Kerberos authentication.

Because of dependencies on the underlying operating system, Windows Server 2008 templates can only be assigned to CAs that also run on Windows Server 2008. Additionally, only Windows Vista client computers and Windows Server 2008 computers can enroll for V3 certificate templates.

|  |  |  |
| --- | --- | --- |
| **Template** | **Windows version required to modify a template** | **Windows version of the CA where the template can be assigned** |
| V1 Template | n/a (Since V1 templates are static) | Windows Server 2000 Enterprise Edition  Windows Server 2003 Enterprise Edition  Windows Server 2008 |
| V2 Template | Windows Server 2003  Windows XP  Windows Server 2008 | Windows Server 2003 Enterprise Edition  Windows Server 2008 Enterprise Edition |
| V3 Template | Windows Server 2008 | Windows Server 2008 |

One important change in Windows Server 2008 and Windows Vista is the addition of Cryptography Next Generation (CNG). CNG supports Suite-B algorithms, making it possible to use alternate and customized cryptographic algorithms for encryption and signing certificates.

Federated Rights Management in Windows Server 2008

Collaboration is a vital part of conducting business today, especially the sharing of information with colleagues and trusted business partners across organizational boundaries. Traditional perimeter security methods do not offer the granular protection needed to safeguard important data and information during inter-company collaboration. The Microsoft Identity and Access platform offers such comprehensive information protection, providing persistent protection from unauthorized use regardless of where that information travels. This helps to mitigate risks while enabling compliance and uninterrupted collaboration.

Windows Server 2008 Active Directory Rights Management Services (AD RMS) helps prevent unauthorized access and use of documents, data and emails. It enables document owners to identify authorized users and manage restrictions on the usage of documents.

Windows Server 2008 enables a new way to protect sensitive information that is both more comprehensive and easier to administer. As in Windows Server 2003, Active Directory Federation Services (AD FS) enables one organization to set up a federated trust with another organization. Users sign on once—to their local domain—and gain access to a partner domain through identity and access federation. Because AD RMS has been integrated with AD FS in Windows Server 2008, a federated trust now allows AD RMS to grant appropriate RMS permissions to an external user without requiring him or her to sign in locally or have his or her own AD RMS server.

This scenario is called “secure federated collaboration.” In essence, an administrator inside a company with a need to share RMS-protected information no longer needs to maintain separate usernames and passwords for external users. External users experience a single sign-on (SSO) that enables them to access RMS-protected content as appropriate without the need to keep track of multiple identities. In short, sharing confidential information securely—whether with partners, suppliers or customers—has become much easier.

AD RMS in Windows Server 2008 works with many applications and across platforms, providing tightly integrated usage rights and encryption that follow content wherever it goes. It can be used to protect documents, spreadsheets, intranet sites, and e-mail. It also provides the tools necessary for developers to integrate RMS functionality with non-RMS-enabled applications. Also, organizations can create custom usage rights templates that can be applied instantly.

## Cryptography Next Generation (CNG)

Cryptography Next Generation (CNG) provides a flexible cryptographic development platform allowing IT Professionals to create, update, and use custom cryptography algorithms in cryptography-related applications, such as Active Directory Certificate Services, Secure Sockets Layer (SSL), and Internet Protocol security (IPsec). CNG implements the U.S. government's Suite B cryptographic algorithms, which include algorithms for encryption, digital signatures, key exchange, and hashing.

CNG provides a set of APIs that are used to perform basic cryptographic operations, such as creating, storing, and retrieving cryptographic keys. It also supports the installation and use of additional cryptographic providers. CNG enables organizations and developers to use either their own cryptographic algorithms, or implementations of standard cryptographic algorithms.

CNG supports the current set of CryptoAPI 1.0 algorithms and also provides support for elliptic curve cryptography (ECC) algorithms. A number of ECC algorithms are required by the United States government’s Suite B effort.

For more information about Suite B, see: <http://www.nsa.gov/ia/industry/crypto_suite_b.cfm>

## Read-Only Domain Controllers

A Read-Only Domain Controller (RODC) is a new type of domain controller available in the Windows Server 2008 operating system, designed primarily to be deployed in remote locations. RODC is covered in detail in the Remote Locations section of this paper.

## Server and Domain Isolation

In a Microsoft Windows-based network, administrators can logically isolate server and domain resources to limit access to only trusted, managed computers. Server and Domain Isolation (SDI) creates a logical separation of network devices based on policy. SDI maintains restricted access to confidential servers and machines on the network. For example, a logical network can be created inside the existing physical network, where computers share a common set of requirements for secure communications. Each computer in this logically isolated network must provide authentication credentials to other computers in the isolated network to establish connectivity.

This isolation prevents unauthorized computers and programs from gaining access to resources inappropriately. Requests from computers that are not part of the isolated network are ignored. Server and domain isolation can help protect specific high-value servers and data as well as protect managed computers from unmanaged or rogue computers and users.

Two types of isolation can be used to protect a network:

* Server isolation ‑ In a server isolation scenario, specific servers are configured using IPsec policy to accept only authenticated communications from other computers. For example, the database server can be configured to accept connections from the Web application server only.
* Domain isolation **‑** To isolate a domain, administrators can use Active Directory domain membership to ensure that computers that are members of a domain accept only authenticated and secured communications from other computers that are domain members. The isolated network consists of only computers that are part of the domain. Domain isolation uses IPsec policy to provide protection for traffic sent between domain members, including all client and server computers.

**Summary**

With Windows Server 2008, organizations can benefit from unprecedented security using the policy based security features, such as Network Access Protection. Evaluating and controlling the health and security status of connecting computers will provide significant security improvements for organization. The new management interfaces in Windows Server 2008 simplify the administrative process of configuring and maintaining multiple servers within the organization, thereby reducing the costs of managing the enterprise’s network security.

# Remote Locations

## Introduction

Businesses want to get closer to their customers, and are moving workers away from central locations and out to remote locations like branch offices. With the growing number of remote locations, the IT management needs and security concerns for these locations also grows proportionally. Microsoft recognizes this rapidly-growing part of the workforce, and the need for new solutions to deal with the challenges specific to branch offices.

Because remote locations have little or no IT staff onsite, servers in these locations pose several concerns for IT managers. Software running on servers must utilize the lower-speed WAN connections effectively without consuming all bandwidth, slowing down mission-critical data transfer, or degrading application experiences for users in these remote locations. Security is a greater concern at remote locations because the physical security of the server cannot always be guaranteed. With the majority of the IT staff offsite, server solutions that provide centralized management, as well as remote administration and deployment, are preferred for a branch office or remote location.

Microsoft began addressing the needs and challenges of the branch office scenario in Windows Server 2003 R2. The release of Windows Server 2008 includes many additional improvements that will give administrators greater control over remote locations and increase the level of protection of both the remote site and the organization’s central network and data. It also provides a greater degree of flexibility for IT Professionals needing to meet the unique needs of their organization.

For remote locations, Windows Server 2008 provides important benefits that can be divided into three categories:

* Improving the efficiency of remote server deployment and administration
* Reducing security risks in remote locations like branch offices
* Improving the efficiency of WAN communications and bandwidth utilization

The enhanced and improved TCP/IP stack used in Windows Server 2008 networking improves performance by automatically tuning network connections to maximize throughput. It increases scalability though optimized support for multi-gigabit networks and next generation Internet protocols to meet the growing IT infrastructure demands. Windows Server 2008 networking boosts security through seamlessly integrated network security features to provide a solid foundation for business workloads. For workers in remote locations, the new TCP/IP stack will increase efficiency by providing better transfer times and reducing latency issues with WAN connections.

Windows Server 2008 addresses the fundamental remote location needs with a variety of new features and enhancements by providing simplified deployment and effective management of vital server roles, improved security, and an architecture that optimizes performance and provides for service continuity.

## Deployment and Administration

Managing the servers, services, and security at remote locations is an ongoing challenge for IT Professionals. Windows Server 2008 simplifies remote deployment and ongoing administration of the servers located in branch offices.

Changes and enhancements of Active Directory directory service, the introduction of the Read-Only Domain Controller, BitLocker, role separation, and the Server Core installation option are specific Windows Server 2008 features that address the unique needs of the branch office and increase the effectiveness of IT departments managing remote locations.

## Read-Only Domain Controllers

A Read-Only Domain Controller (RODC) is a new type of domain controller available in the Windows Server 2008 operating system. RODC is designed primarily to be deployed in branch office environments. With an RODC, organizations can limit the risks of deploying a domain controller in locations, such as branch offices, where physical security cannot be guaranteed.

Except for account passwords, an RODC holds all of the Microsoft Active Directory Domain Services (AD DS) objects and attributes that a writable domain controller holds. Clients, however, are not able to write changes directly to a RODC. Because no changes are written directly to the RODC and therefore do not originate locally, writable domain controllers that are replication partners do not have to pull changes from the RODC. This reduces the workload of bridgehead servers in the hub site and the effort required to monitor replication.

Administrator role separation specifies that any domain user can be delegated to be the local administrator of an RODC without granting that user any user rights for the domain itself or other domain controllers. This creates a scenario where a local branch user can log on to an RODC to perform maintenance work on the server, such as upgrading a driver, without having access to domain resources outside the branch.

## BitLocker Drive Encryption

BitLocker Drive Encryption is a new security feature in Windows Server 2008 that helps to protect servers in branch offices. It is also available in Windows Vista Enterprise and Windows Vista Ultimate editions for protecting client computers and mobile computers for roaming users. BitLocker encrypts the contents of a disk drive.

BitLocker enhances data protection by bringing together two major sub-functions: system volume encryption and integrity-checking for early-boot components. The entire system volume is encrypted, including the swap and hibernation files, which increases the security of the remote servers in the branch office location. BitLocker addresses the threats of data theft or exposure from a lost, stolen, or inappropriately decommissioned PC. In the branch office scenario, this is important because the physical security of the server cannot always be guaranteed.

## Server Core

Server core is a minimal installation of Windows Server that provides specific functionality without any unneeded features. Server Core is covered in detail in the Server Management section of this paper.

## Enhanced Manageability of Active Directory

Windows Server 2008 includes improvements in Active Directory Domain Services (AD DS) that simplify the management of Domain Services and provide administrators with a greater degree of flexibility to address the needs of branch offices. Some management enhancements include:

* An updated AD DS Installation Wizard
* Changes to the Microsoft Management Console used to manage AD DS
* New installation options for domain controllers
* Updated installation wizard that simplifies the AD DS installation
* Improved interface and management options for AD DS
* Improved tools to find domain controllers through the enterprise

With the new installation wizard, all related functionality is now grouped together, streamlining the process and saving time during deployment. Unattended installation in Windows Server 2008 never requires a response to any user interface prompt, further simplifying remote installations. This also enables the installation of AD DS on a Server Core installation. To ensure that a newly installed DNS server operates correctly, DNS is automatically configured for DNS client settings, forwarders, and root hints as necessary, based on the installation options selected.

These AD DS interface improvements offered in Windows Server 2008 will reduce IT administration time by streamlining the initial deployment simplifying the management of servers in branch locations.

# High Availability

## Introduction

IT departments must ensure that mission-critical applications are always available. High Availability is a central theme in many of the enhancements in Windows Server 2008. Failover Clustering, network load balancing, and new backup and restoration features in Windows Server 2008 combine to provide organizations with a High Availability solution to ensure that mission-critical applications, services and information remain available with minimal downtime to all users.

## Failover Clustering

A failover cluster, formerly known as a server cluster, is a group of independent computers that work together to increase the availability of applications and services. The clustered servers, called nodes, are connected by physical cables as well as by software. If one of the cluster nodes fails, through a process known as failover, another node in the cluster will take over for the failed node ensuring that users experience a minimal disruption in service. Failover clusters are used by IT Professionals who must provide high availability for mission critical services and applications.

In Windows Server 2008, the improvements to failover clusters are aimed at simplifying clusters, making them more secure, and enhancing cluster stability.

Cluster setup and configuration is simplified in Windows Server 2008, with a new validation wizard that lets users confirm that the system, storage, and network configuration are suitable for a cluster. Some of the tests performed by the new validation wizard include:

* Node tests ‑ Confirm that the servers are running the same operating system version and have the same software updates
* Network tests ‑ Determine whether the planned cluster network meets specific requirements, such as having at least two separate subnets for network redundancy
* Storage tests ‑ Analyze whether the storage is correctly configured so that all cluster nodes have access to all shared disks and meet specified requirements.

Windows Server 2008 includes support for global unique identifier, or GUID Partition Table (GPT) disks in cluster storage. GPT disks can have partitions larger than two terabytes and have built-in redundancy, unlike master boot record (MBR) disks. GPT offers more advantages than master boot record (MBR) partitioning because it allows up to 128 partitions per disk, provides support for volumes up to 18 exabytes in size, allows primary and backup partition tables for redundancy, and supports unique disk and partition IDs.

To simplify cluster management, the management interfaces is improved to allow administrators to focus on managing their applications and data, not their cluster. The new interface is task-based and more intuitive, and is supported by wizards that guide administrators through what were previously complex operations.

Windows Server 2008 failover clusters provide better functionality and reliability than in previous releases of server clusters. Improvements include:

* Dynamic addition of disk resources **‑** Resource dependencies can be modified while resources are online, which means administrators can make additional disk storage available without interrupting the applications that will use it.
* Improved performance and stability with data storage **‑** When a failover cluster communicates with a Storage Area Network (SAN) or direct attached storage (DAS), it uses the least disruptive commands; there are fewer SCSI bus resets. Disks are never left in an unprotected state, meaning that the risk of volume corruption is reduced. Failover clusters also support improved methods for disk discovery and recovery. Failover clusters support three types of storage connections: Serial Attached SCSI (SAS), iSCSI, and Fibre Channel.
* Easier disk maintenance **‑** Maintenance mode is significantly improved, so that administrators can run tools to check, fix, back up, or restore disks more easily, and with less disruption to the cluster.

For administrators using clusters to deliver a high availability solution, Windows Server 2008 simplifies the deployment and management of clusters and improves the performance and reliability.

## Clustering and Hyper-V

Windows Server 2008 Failover Clustering provides high availability for Hyper-V by allowing virtual machines to migrate to other nodes in the cluster during downtime. Clustering can be achieved by clustering the Hyper-V role itself (Host Clustering), or by clustering the individual virtual machines running in Hyper-V (Guest Clustering).

Using Windows Server 2008 Failover Clustering to make the Hyper-V role highly available means that two or more servers running Hyper-V have the Failover Clustering role added, and are configured in a supported cluster configuration. This is known as Host Clustering. A key requirement of Windows Server 2008 Failover Clustering is shared storage for the cluster nodes. This can include an iSCSI or Fiber-Channel Storage Area Network (SAN). All virtual machines are stored in the shared storage area, and one of the Hyper-V nodes manages the running virtual machine. When planned downtime occurs, the Failover Clustering service can move affected virtual machines to another cluster node. When unplanned downtime occurs, the Failover Clustering service will automatically restart virtual machines on a surviving cluster node. Host Clustering provides high availability for the entire Hyper-V platform and for all virtual machines hosted on a Hyper-V server.

Host Clustering can help prevent unplanned downtime, and can also keep virtual machines available during Hyper-V host maintenance. Host Clustering also helps datacenters respond to changing workloads by allowing Hyper-V administrators to migrate running virtual machines to hosts with available resources using the Quick Migration feature.

Virtual machines running in Hyper-V can be clustered, even if the underlying host operating system is not. Hyper-V allows virtual machines to access external storage using iSCSI. Two or more virtual machines can be configured so that the guest operating systems in those VMs access external shared storage where a cluster resource is stored. If the guest operating systems support clustering, then they can be configured to provide high availability for the cluster resource.

Hyper-V Guest Clustering can be used to provide high availability for a large variety of resources including databases, file shares, network infrastructure, and application services. Hyper-V Guest Clustering can be combined with Windows Server 2008 Network Load Balancing (NLB) services to provide both high availability and load balancing across multiple Hyper-V host servers. For example, Hyper-V virtual machines can be used to host a Web server farm or Terminal Services farm. NLB balances traffic so that no single VM is overloaded with requests, individual VMs within the farm can be rebooted without disrupting client access, and a new server in the farm can be easily provisioned using VM templates.

Windows Server 2008 clustering is enhanced to remove design constraints for Multi-site clustering. The less than 500ms latency requirement of Windows Server 2003 clusters is removed. The latency requirement of Windows Server 2008 is configurable. In Windows Server 2008, clusters can now cross subnets. This removes a previous requirement to use a VLAN to connect disparate sites. Multi-site clustering in Windows Server 2008 makes it possible to provide failover of datacenter operations to a recovery site that is geographically separate from the primary site.

## Network Load Balancing

Network Load Balancing (NLB) is a feature that distributes the load for networked client and server applications across multiple servers in an NLB cluster. NLB is important for organizations that need to distribute client requests across a set of servers. It is particularly useful for ensuring that stateless applications, such as a Web based applications running on Internet Information Services, can be scaled out by adding additional servers as the work load increases. NLB provides scalability by allowing additional servers to be added as load increases. NLB provides reliability by allowing users to easily replace a malfunctioning server. Enhancements to NLB in Windows Server 2008 include:

* Support for IPv6 ‑ NLB fully supports IPv6 for all communication.
* Support for NDIS 6.0 ‑ NDIS 6.0 is the next major version of the Network Driver Interface Specification (NDIS) library. NDIS specifies a standard interface between kernel-mode network drivers and the operating system. The NLB driver has been completely rewritten to use the new NDIS 6.0 lightweight filter model. NDIS 6.0 retains backward compatibility with earlier NDIS versions. Improvements in the design of NDIS 6.0 include enhanced driver performance and scalability and a simplified NDIS driver model.
* WMI Enhancements ‑ The WMI enhancements to the MicrosoftNLB namespace are for IPv6 and multiple dedicated IP address support.
* Classes in the MicrosoftNLB namespace ‑ support IPv6 addresses (in addition to IPv4 addresses).
* The MicrosoftNLB\_NodeSetting class ‑ supports multiple dedicated IP addresses by specifying them in DedicatedIPAddresses and DedicatedNetMasks.
* Enhanced functionality with Internet Security and Acceleration (ISA) Server ‑ ISA Server can configure multiple dedicated IP addresses for each NLB node for scenarios where clients consist of both IPv4 and IPv6 traffic. Both IPv4 and IPv6 clients need to access a particular ISA Server to manage the traffic. ISA can also provide NLB with SYN attack and timer starvation notifications (these scenarios typically occur when a computer is overloaded, or is being infected by an Internet virus).
* Support for multiple dedicated IP addresses per node ‑ NLB fully supports defining more than one dedicated IP address per node (previously, only one dedicated IP address per node was supported), allowing multiple applications to be hosted on the same NLB cluster in scenarios where separate applications require their own dedicated IP address.

These features provide support for new industry standards, increased performance, enhanced interoperability, better security, and more flexibility and for application deployment and consolidation.

## Windows Backup

Backup is another important component of Windows Server 2008 that is designed to provide high availability of services. The Backup feature provides a backup and recovery solution for the server on which it is installed. It introduces new backup and recovery technology, replacing the previous Backup feature that was available with earlier versions of the Windows operating system.

The Backup feature can be used to protect the entire server efficiently and reliably without worrying about the intricacies of backup and recovery technology. Simple wizards guide the user through setting up an automatic backup schedule, creating manual backups if necessary, and recovering items or entire volumes. Backup in Windows Server 2008 can be used to back up an entire server or selected volumes.

Backup uses Volume Shadow Copy Service and block-level backup technology to efficiently back up and recover the operating system, files and folders, and volumes. After the first full backup is created, Backup automatically runs incremental backups by saving only the data that has changed since the last backup occurred. Unlike previous versions, administrators no longer have to worry about manually scheduling full and incremental backups.

Restoration is improved and simplified with Windows Server 2008. Items can now be restored by choosing a backup from which to recover, and then selecting items to restore. Specific files or all of the contents of a folder can be recovered. With regard to incremental backups, previously, if an item was stored on an incremental backup, it was necessary to manually restore from multiple backups. Now, the user can simply choose the date on which the version they want to restore was backed up.

Windows Server 2008 provides the backup and recovery solutions needed to complete a high-availability solution that protects both the organization’s data and the operating systems on the servers in the network. It also eases the administrative burden of ensuring mission-critical data is properly backed up, while speeding data recovery.

# Summary

Microsoft Windows Server 2008 represents the next generation of Windows Server. Windows Server 2008 gives IT Professionals more control over their server and network infrastructure, providing a solid foundation for their business workloads. It increases security by hardening the operating system and protecting the network environment. It also provides IT Professionals with flexibility, speeds up deployment and maintenance of IT systems, makes consolidation and virtualization of servers and applications easier, and provides intuitive administrative tools. Windows Server 2008 also enables organizations to deliver rich Web-based experiences efficiently and effectively, and is a powerful Web Application and Services Platform. Windows Server 2008 provides the best foundation for any organization’s server and network infrastructure.