

Windows Server 2008 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

[Chapter 1: Introduction 8](#_Toc187046928)

[Overview 8](#_Toc187046929)

[Web and Applications 8](#_Toc187046930)

[Virtualization 8](#_Toc187046931)

[Security and Compliance 9](#_Toc187046932)

[Solid Foundation for Business Workloads 9](#_Toc187046933)

[Chapter 2: Server Virtualization with Hyper-V 10](#_Toc187046934)

[Introduction 10](#_Toc187046935)

[Hyper-V Architecture 11](#_Toc187046936)

[Hypervisor Based Virtualization 11](#_Toc187046937)

[Hyper-V Processor Support 14](#_Toc187046938)

[New Hardware Sharing Architecture 15](#_Toc187046939)

[Storage Features 17](#_Toc187046940)

[Robust Networking 18](#_Toc187046941)

[Flexible Role-based Security 19](#_Toc187046942)

[Hyper-V on Server Core 20](#_Toc187046943)

[Flexible Resource Control 21](#_Toc187046944)

[Hyper-V High Availability 22](#_Toc187046945)

[Management Features 24](#_Toc187046946)

[Scenario: Consolidate Infrastructure, Application, and Remote Server Workloads 26](#_Toc187046947)

[Key Consolidation Features 27](#_Toc187046948)

[Scenario: Automate and Consolidate Software Test and Development Environments 28](#_Toc187046949)

[Scenario: Business Continuity and Disaster Recovery 30](#_Toc187046950)

[Scenario: Enabling the Dynamic Datacenter 31](#_Toc187046951)

[MSC Integration 31](#_Toc187046952)

[Virtualization Beyond the Server 32](#_Toc187046953)

[Summary 33](#_Toc187046954)

[Chapter 3: Presentation Virtualization with TS RemoteApp 34](#_Toc187046955)

[Introduction 34](#_Toc187046956)

[Terminal Services RemoteApp 34](#_Toc187046957)

[Terminal Services 35](#_Toc187046958)

[Remote Desktop Connection 6.0 and later 35](#_Toc187046959)

[Plug and Play Device redirection 38](#_Toc187046960)

[Windows Embedded for Point of Service device redirection 38](#_Toc187046961)

[Single Sign-On (SSO) 39](#_Toc187046962)

[TS Session Broker 39](#_Toc187046963)

[Printing Enhancements 40](#_Toc187046964)

[TS Easy Print 40](#_Toc187046965)

[Licensing Improvements 40](#_Toc187046966)

[Terminal Services Gateway (TS Gateway) 42](#_Toc187046967)

[TS Gateway Management 43](#_Toc187046968)

[TS Gateway Functionality 43](#_Toc187046969)

[Terminal Services Web Access 45](#_Toc187046970)

[Improved Web experience 46](#_Toc187046971)

[TS Remote Programs List is dynamically updated 46](#_Toc187046972)

[The Terminal Services Remote Programs Web Part 47](#_Toc187046973)

[Summary 47](#_Toc187046974)

[Chapter 4: Remote Locations 47](#_Toc187046975)

[Introduction 47](#_Toc187046976)

[Deployment and Administration 48](#_Toc187046977)

[Enhanced Manageability of Active Directory 48](#_Toc187046978)

[Read-Only Domain Controllers (RODC) 49](#_Toc187046979)

[Read-only Domain Name System 52](#_Toc187046980)

[Server Virtualization with Hyper-V 53](#_Toc187046981)

[Remote Management and Security Enhancements 53](#_Toc187046982)

[Introduction to Server Core 53](#_Toc187046983)

[BitLocker Drive Encryption 53](#_Toc187046984)

[Enterprise Class Printer Management 54](#_Toc187046985)

[Windows PowerShell 54](#_Toc187046986)

[Windows Remote Management 54](#_Toc187046987)

[Improving WAN Efficiency 55](#_Toc187046988)

[TCP/IP Stack 55](#_Toc187046989)

[Internet Protocol Version 6 (IPv6) 59](#_Toc187046990)

[Quality of Service 59](#_Toc187046991)

[SYSVOL and Distributed File System Replication (DSFR) 60](#_Toc187046992)

[Server Message Block 2.0 61](#_Toc187046993)

[Summary 63](#_Toc187046994)

[Chapter 5: Security and Compliance 64](#_Toc187046995)

[Introduction 64](#_Toc187046996)

[Windows Firewall Advanced Security 65](#_Toc187046997)

[BitLocker Drive Encryption 67](#_Toc187046998)

[Active Directory Domain Services: Auditing 67](#_Toc187046999)

[Auditing AD DS access 68](#_Toc187047000)

[Auditing AD DS Changes 68](#_Toc187047001)

[Global audit policy 69](#_Toc187047002)

[Service-based AD DS 70](#_Toc187047003)

[Read-Only Domain Controllers (RODCs) 70](#_Toc187047004)

[Server and Domain Isolation 70](#_Toc187047005)

[Enterprise PKI 71](#_Toc187047006)

[Enterprise CA Management with PKIView 72](#_Toc187047007)

[Certificate Services 73](#_Toc187047008)

[Certificate Web Enrollment 73](#_Toc187047009)

[Network Device Enrollment 74](#_Toc187047010)

[Managing Certificates with Group Policy 75](#_Toc187047011)

[Certificate-related Group Policy Settings 76](#_Toc187047012)

[Managing peer trust and trusted root CA stores 76](#_Toc187047013)

[Managing trusted publishers and blocking unwanted certificates 77](#_Toc187047014)

[Certificate Deployment Changes 77](#_Toc187047015)

[Online Certificate Status Protocol Support 78](#_Toc187047016)

[Functionality Provided by OCSP 79](#_Toc187047017)

[Group Policy Settings for OSCP 80](#_Toc187047018)

[V3 Certificate Templates 80](#_Toc187047019)

[Cryptography Next Generation (CNG) 81](#_Toc187047020)

[Identity and Access Management in Windows Server 2008 82](#_Toc187047021)

[Active Directory Rights Management Services 84](#_Toc187047022)

[Active Directory Federation Services 85](#_Toc187047023)

[Persistent Information Protection 85](#_Toc187047024)

[Scenario: Secure and Easy Collaboration 86](#_Toc187047025)

[Federated Rights Management Summary 86](#_Toc187047026)

[Other security enhancements 87](#_Toc187047027)

[Code integrity 87](#_Toc187047028)

[Windows Service Hardening 87](#_Toc187047029)

[Windows Server Core 88](#_Toc187047030)

[Removable device installation 88](#_Toc187047031)

[Network Access Protection (NAP) 88](#_Toc187047032)

[An Introduction to Network Access Protection? 88](#_Toc187047033)

[NAP architecture 89](#_Toc187047034)

[NAP components 90](#_Toc187047035)

[Client computer health 93](#_Toc187047036)

[NAP Administration server 93](#_Toc187047037)

[Network Policy Server (NPS) 94](#_Toc187047038)

[Example: How NAP Enforcement Works 94](#_Toc187047039)

[NAP enforcement methods 96](#_Toc187047040)

[Summary 98](#_Toc187047041)

[Chapter 6: Web & Applications 98](#_Toc187047042)

[Introduction 98](#_Toc187047043)

[Internet Information Services (IIS) 7.0 99](#_Toc187047044)

[Modular Design 100](#_Toc187047045)

[Increased Extensibility 100](#_Toc187047046)

[Distributed Configuration 101](#_Toc187047047)

[Administration Tools 102](#_Toc187047048)

[New IIS Manager 102](#_Toc187047049)

[Diagnostics and Troubleshooting 104](#_Toc187047050)

[Windows Process Activation Service (WAS) 106](#_Toc187047051)

[Windows System Resource Manager (WSRM) 107](#_Toc187047052)

[Eventing Infrastructure 107](#_Toc187047053)

[Events in Windows Server 2008 and Windows Vista 107](#_Toc187047054)

[New Ways to View Events 108](#_Toc187047055)

[XML Structure 109](#_Toc187047056)

[Event Subscriptions 109](#_Toc187047057)

[The Restart Manager 109](#_Toc187047058)

[Microsoft .NET Framework 3.0 110](#_Toc187047059)

[Windows Communication Foundation (WCF) 111](#_Toc187047060)

[Windows Presentation Foundation (WPF) 112](#_Toc187047061)

[Windows Workflow Foundation (WF) 112](#_Toc187047062)

[Windows CardSpace 112](#_Toc187047063)

[Service Trace Viewer Tool (SvcTraceViewer.exe) 112](#_Toc187047064)

[PHP Support 113](#_Toc187047065)

[Certificate Services 113](#_Toc187047066)

[Windows Media Services 113](#_Toc187047067)

[Summary 114](#_Toc187047068)

[Chapter 7: Server Management 115](#_Toc187047069)

[Introduction 115](#_Toc187047070)

[Initial Configuration Tasks 115](#_Toc187047071)

[Server Manager Console 118](#_Toc187047072)

[Managing the roles, role services and features installed on the server 118](#_Toc187047073)

[What are server roles and role services? 118](#_Toc187047074)

[What are features? 119](#_Toc187047075)

[Server Manager Wizards 122](#_Toc187047076)

[Server Manager Command-Line Tools 124](#_Toc187047077)

[Windows PowerShell 125](#_Toc187047078)

[Consistency and Ease of Use 125](#_Toc187047079)

[Interactive and Scripting Environments 125](#_Toc187047080)

[Object Orientation and .NET Framework 126](#_Toc187047081)

[Group Policy Preferences 126](#_Toc187047082)

[Preferences vs. Policy Settings 127](#_Toc187047083)

[Group Policy Preference Items 129](#_Toc187047084)

[Group Policy Preference Features 132](#_Toc187047085)

[Targeting Control 132](#_Toc187047086)

[Deploying Group Policy Preferences 133](#_Toc187047087)

[Benefits of Group Policy Preferences 134](#_Toc187047088)

[Windows Remote Management (WS-Management) 135](#_Toc187047089)

[Windows Remote Shell 136](#_Toc187047090)

[Server Core 136](#_Toc187047091)

[Not an Application Platform 137](#_Toc187047092)

[Enterprise Class Print Management 138](#_Toc187047093)

[Managing Printers 138](#_Toc187047094)

[Listing and Removing Printers in Active Directory 139](#_Toc187047095)

[Deploying Printers by Using Group Policy 139](#_Toc187047096)

[Troubleshooting Printers 139](#_Toc187047097)

[Key Benefits 140](#_Toc187047098)

[Windows Deployment Services 140](#_Toc187047099)

[Enhancements to Windows Deployment Services 141](#_Toc187047100)

[New Active Directory Domain Services Installation Wizard 141](#_Toc187047101)

[Restartable Active Directory Domain Services (AD DS) 143](#_Toc187047102)

[Active Directory Domain Services Snapshot Viewer 145](#_Toc187047103)

[Summary 145](#_Toc187047104)

[Chapter 8: High Availability 146](#_Toc187047105)

[Introduction 146](#_Toc187047106)

[Failover Clustering 147](#_Toc187047107)

[New Functionality in failover clustering 147](#_Toc187047108)

[Enhanced scalability for large volumes 147](#_Toc187047109)

[Improvements in failover clusters 148](#_Toc187047110)

[Improved Stability 149](#_Toc187047111)

[Storage integration 150](#_Toc187047112)

[Networking and security 150](#_Toc187047113)

[Clustering and Hyper-V 151](#_Toc187047114)

[Network Load Balancing 152](#_Toc187047115)

[Windows Backup 153](#_Toc187047116)

[New Backup functionality 154](#_Toc187047117)

[Windows Reliability and Performance Monitor 154](#_Toc187047118)

[New monitoring features 155](#_Toc187047119)

[Policy-based Quality of Service 157](#_Toc187047120)

[Summary 157](#_Toc187047121)

[Chapter 9: Summary 158](#_Toc187047122)

# Chapter 1: 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 help save time, reduce costs, and provide a platform for a dynamic datacenter. Powerful new tools like Internet Information Server 7.0 (IIS 7.0), Windows Server Manager, and Windows Server 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 provides organizations with the ability to deliver rich Web-based experiences efficiently and effectively.

The release of Internet Information Server 7.0 (IIS 7.0) as part of Windows Server 2008 offers improved administration and diagnostics, better development and application tools, and lower infrastructure costs. It is also a completely modular, extensible Web server with expanded application hosting, which retains excellent compatibility in solving key customer challenges.

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. Server virtualization with 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, such as failover clustering, to provide high availability and Network Access Protection (NAP) to quarantine noncompliant 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 more information, see: Chapter 3: Presentation Virtualization with Terminal Services RemoteApp.

## 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 BitLocker™.

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 Server Core, PowerShell, Windows Deployment Services, and enhanced networking and clustering technologies, Windows Server 2008 provides the most versatile and reliable Windows 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 install Windows components from removable media, such as CD or DVD. The Windows PowerShell command-line shell and scripting language helps IT Professionals automate common tasks and more easily control system administration and 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 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 a new implementation of the TCP/IP protocol stack, known as the Next Generation TCP/IP stack. The Next Generation TCP/IP stack meets the connectivity and performance needs of today’s varied networking environments and technologies through a complete redesign of the TCP/IP stack.

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 clusters, making them easier to secure, and more stable.

# Chapter 2: Server Virtualization with Hyper-V

## Introduction

Today's datacenter is a complex ecosystem where different kinds of servers, operating systems, and applications interact with a wide variety of desktop and mobile clients. IT departments are under increasing pressure to manage and support this assortment of mission-critical technologies while controlling costs and maintaining reliability and security. Deploying server virtualization technology—moving disparate servers to virtual machines (VMs) in a centrally managed environment—is an increasingly popular option for addressing these challenges.

Virtualization helps reduce IT costs, centralize network management, increase network security, improve server availability, and to increase hardware utilization.

Windows Server 2008 includes Hyper-V, a powerful virtualization and network management technology that enables businesses to take advantage of virtualization's benefits without buying third-party software. Virtual machines provide unprecedented abilities to leverage available hardware, Microsoft and its partners provide one-stop support for interoperability issues with multiple operating systems (Windows, Linux, and Xen-enabled Linux), and IT departments can manage both virtual and physical resources using flexible and powerful tools.

This chapter introduces Hyper-V as a key component of the Microsoft desktop-to-datacenter virtualization strategy. It shows how new and enhanced features in Hyper-V help relieve enterprise customer pain points in common scenarios: server consolidation, business continuity/disaster recovery management, testing and development, and the dynamic data center. It also highlights how these benefits scale to meet the unique needs of small and branch offices.

Virtualization is a widely adopted solution. 80 percent of organizations are using or evaluating virtualization and seeing its advantages for server consolidation, centralized management, and other cost-saving uses. Because these benefits decrease cost, companies want to virtualize more demanding workloads. They want more powerful and flexible virtualization solutions that are better integrated with their management tools. Wide adoption of 64-bit, multi-processor, multi-core servers spurs demand for virtual machines that are better able to take advantage of more robust processing power.

In response to these developments, Microsoft created Hyper-V, a next-generation, 64-bit virtualization technology facilitating agility and seamless management of both physical and virtual components. It provides a platform enabling flexibility through dynamic and reliable virtualization capabilities.

## Hyper-V Architecture

### Hypervisor Based Virtualization

Hyper-V was designed using a 64-bit hypervisor. The hypervisor is a thin layer of software that resides between the operating system and the hardware. The hypervisor allows multiple virtual machines (VMs) to access physical memory and CPU resources without conflicts. In combination with virtualization-aware hardware that includes processors using Intel VT and AMD “Pacifica” technology, the Hyper-V hypervisor enables high performance and nearly limitless scalability for guest operating systems.

#### Hardware Virtualization

Because the Hyper-V hypervisor takes advantage of Intel VT and AMD “Pacifica” technology, more of the work of virtualizing multiple operating systems is performed by system hardware and less needs to be performed by the virtualization stack and hypervisor.

Virtualization platforms that rely on software emulation of hardware must frequently interrupt guest operating systems by performing on-the-fly translation of hardware requests into a form that is compatible with the virtualization environment. Intel VT and AMD “Pacifica” hardware technology render much of this on-the-fly translation unnecessary by incorporating virtualization extensions to the x86 architecture. This means that virtualization platforms that are designed for VT and “Pacifica” have lower overhead, and virtual machines run more efficiently. This collaboration between hardware virtualization features and the software virtualization components of Hyper-V creates a high-performance virtualization platform.

#### 64-bit Architecture

The Hyper-V hypervisor is a 64-bit design. Hyper-V must be run on 64-bit editions of Windows Server 2008, and provides nearly unlimited scalability for virtual machines. The 64-bit architecture of Hyper-V can address far more memory than virtualization platforms based on 32-bit architectures, Hyper-V host server can accommodate up to 1 Terabyte of physical RAM.

Virtual machines hosted by Hyper-V can be assigned up to 64 Gigabytes (GB) of RAM each. The dynamic hardware assignment feature of Hyper-V, discussed later in this chapter, allows a variable amount of RAM—up to 64 GB—to be assigned to each virtual machine based on that virtual machine’s resource needs. This allows more demanding workloads to be virtualized so that organizations can take full advantage of the ability to host multiple guest operating systems and VMs. With this flexibility in resource assignment, multiple guest operating systems can be consolidated on a single Hyper-V host, each running with little compromise in efficiency.

#### 64-bit Guest Operating System Support

The 64-bit hypervisor used in Hyper-V supports both 32-bit and 64-bit guest operating systems. Some applications may be available only in 32-bit versions and some applications may be available in only 64-bit versions (for example, an LOB application may be available in a 32-bit version while Microsoft Exchange Server 2007 is available only as a 64-bit application). Both 32-bit and 64-bit virtual machines can run alongside each other on the same Hyper-V server. The flexibility to accommodate both 32-bit and 64-bit virtual machines is an important benefit of the Hyper-V hypervisor. The 64-bit hypervisor creates a virtualization foundation that supports any future growth path that an organization wants to follow.

#### Operating System Partitioning

Hyper-V assigns host system hardware resources among multiple VMs using partitions. A partition is a logical division of the host server that contains a single operating system. The parent partition contains a virtualization stack, which manages the memory and virtual devices of child partitions. Child partitions are referred to as virtual machines. With Hyper-V, there is limit of one parent partition (an instance of Windows Server 2008 x64 or a Server Core installation of Windows Server 2008 x64), and an unlimited number of child partitions that can be configured.

The parent partition has ownership of the keyboard, mouse, and video display attached to the Hyper-V host server. The parent partition also contains a Windows Management Instrumentation (WMI) Provider to facilitate management of all aspects of the virtualized environment. In addition, any Independent Hardware Vendor (IHV) drivers needed for host system hardware are contained in the parent partition. The child partition forms a logical container for the operating system, applications, and data files associated with a Virtual Machine. The child partition has limited access to host server hardware, and must access this hardware through a hardware sharing model known as VMBus, which is discussed later in this chapter.

#### Microkernelized Hypervisor Architecture

The Hyper-V hypervisor incorporates the same design principles as microkernel operating systems. The fact that operating system drivers and other components that are exposed to attack are executed at a less privileged level means that a component malfunction or attack results in limited or no damage to the kernel. The Hyper-V hypervisor uses a similar design approach to achieve a minimal Trusted Computing Base (TCB), which incorporates no drivers of its own (these are contained in the parent and child partitions). This microkernelized hypervisor architecture provides a more stable, secure foundation for running virtual machines, especially when compared to virtualization platforms based on a monolithic hypervisor—one that incorporates hardware drivers into the hypervisor codebase. The illustration below shows the Windows Server virtualization architecture.

##### C:\Documents and Settings\Peter\Desktop\WSv.PNG

Figure 1: Hyper-V Architecture

### Hyper-V Processor Support

Modern server hardware offers many processor configuration choices. Multiple sockets on a server motherboard can be populated with processors that feature multiple cores. Hyper-V processor performance scales primarily with the number and speed of processor cores available. For example, two sockets populated with dual-core processors present four processing cores to Hyper-V.

The number of processor sockets that can be used by Hyper-V is determined by the edition of Windows Server 2008 installed. The table below provides some examples of processor support:

Table 1: Example Processor Support by Processor Configuration and Operating System Version

|  |  |  |
| --- | --- | --- |
| **Processor Configuration** | **Parent Partition operating system** | **Result** |
| Two sockets populated with dual-core processors | Windows Server 2008 Standard x64 | * Parent partition utilizes four processor cores * Each child partition can be assigned up to 4 logical processors |
| Eight sockets populated with dual-core processors | Windows Server 2008 Standard x64 | * Parent partition utilizes 16 processor cores * Each child partition can be assigned up to 4 logical processors |
| Two sockets populated with quad-core processors | Windows Server 2008 Enterprise x64 | * Parent partition utilizes eight processor cores * Each child partition can be assigned up to 4 logical processors |
| 16 sockets populated with dual-core processors | Windows Server 2008 Enterprise x64 | * Parent partition utilizes Eight processor cores * Each child partition can be assigned up to 4 logical processors |

Note:

1. Windows Server 2008 Standard Edition x64 is able to utilize up to four processor sockets.
2. Windows Server 2008 Enterprise Edition x64 is able to utilize up to eight processor sockets.
3. Windows Server 2008 Datacenter Edition x64 is able to utilize up to 16 processor sockets in conjunction with Hyper-V.

Hyper-V presents processor cores to virtual machines as logical processors. A server with four sockets populated with quad-core processors contains 16 processing cores. These 16 processing cores can be presented as logical processors to virtual machines. Each virtual machine can be configured with up to four logical processors. Each logical processor translates the virtual machines’ compute load on that logical processor into a thread of execution on a physical processor in the host server.

The table above shows several possible configurations and the resulting processor assignment possibilities in each configuration. The operating system installed in the child partition will determine the number of logical processors that can be utilized by that operating system.

### New Hardware Sharing Architecture

#### VMBus

Hyper-V incorporates a new hardware-sharing architecture based on a cross-partition communication channel known as the VMBus. VMBus is a high speed, point-to-point in memory bus and inter-partition communication mechanism. VMBus is the mechanism that the host and VMs use to communicate with each other. As previously discussed, the hypervisor manages interaction between the host system and VMs as well as the memory and processor of the host server. Disk, networking, input/output, and video hardware interaction is managed by the VMBus.

#### Virtualization Service Providers (VSPs)

Virtualization Service Providers (VSPs) reside in the parent partition and interact with host server hardware on behalf of Virtualization Service Clients (VMs) located in child partitions. VSPs act as multiplexers, allowing multiple child partitions to share hardware. For example, on a Hyper-V host with 10 virtual machines but only one physical network adapter, the VSP in the parent partition ensures that all these virtual machines can successfully and securely share the same NIC. Hyper-V has VSPs for storage, networking, input and video.

#### Virtualization Service Clients (VSCs)

Virtualization Service Clients (VSCs) are drivers in a guest operating system that indirectly access host server hardware by communicating over the VMBus to VSPs in the parent partition. VSCs present a purely synthetic virtual device (this is not an emulated device and is described in more detail later) and communicate by means of VMBus to the corresponding VSP (storage, networking, input, or video) in the parent partition. There are one set of VSPs that run in the parent partition. Each child partition runs its own set of VSCs that communicate with the corresponding VSP in the parent partition.

Hyper-V includes Integration Components, which take the place of the VM Additions used in Microsoft Virtual Server 2005. The VM Additions in Microsoft Virtual Server 2005 were used to enhance the performance of guest operating systems (by patching the guest operating system with virtualization-aware software components) and to provide integration components to support features like clean guest shutdown from the Microsoft Virtual Server management interface. Hardware-assisted virtualization renders guest operating system patching unnecessary. Integration Components perform these tasks in Hyper-V.

#### Synthetic Devices

The VMBus architecture in Hyper-V enables presentation of a new type of hardware to guest operating systems: synthetic devices. Synthetic devices are virtual devices that are mapped to physical devices but do not emulate physical devices. Emulated devices create an exact software representation of a physical device. For example, an emulated disk controller is indistinguishable, to the guest operating system, from its physical counterpart. This means that the guest operating system will also experience the limitations of its physical counterpart.

Synthetic devices are available to all guest operating systems with VSCs available in the Integration Components package for that operating system. In general, guest operating systems based on Windows 2000 Server and later can use synthetic devices. The table below lists synthetic device support for supported guest operating systems.

Table 2: Synthetic Device Availability

|  |  |
| --- | --- |
| **Guest Operating System** | **Virtualized Device Type** |
| Windows Server 2008, Windows Server® 2003 R2, Windows Vista® SP1, Windows® XP SP3  Note: Support for synthetic devices in Windows Vista SP1 and Windows XP SP3 will be present in the release of Hyper-V. | Synthetic |
| Other Windows operating systems | Emulated |
| SUSE Linux Enterprise 10 | Synthetic |
| Other Linux operating systems | Emulated |

### Storage Features

Hyper-V introduces several new features related to virtual machine storage hardware. In Microsoft Virtual Server, the file contents of a virtual machine are stored in one or more Virtual Hard Drive (VHD) files. The host operating system maintained these VHD files on an accessible file system, typically internal hard-drive storage, or a Storage Area Network (SAN). Hyper-V supports new ways of accessing storage for guest operating systems.

#### Pass-Through Disk Access for Virtual Machines

Pass-Through Disk Access allows a virtual machine to directly access a writeable file system without using a VHD file. For example, a virtual machine running Windows Server 2008 with a SQL Server® database could use Pass-Through Disk Access to access database files located on an iSCSI or Fiber-Channel SAN. This virtual machine could also be configured to access a partition on a disk directly attached to the Hyper-V host server.

Using Pass-Through Disk Access makes data that would ordinarily be encapsulated in the VHD format available for manipulation on a file system accessible by non-virtualized systems. This additional choice in storage configuration adds flexibility to Hyper-V use scenarios. For example, a virtualized SQL Server might store its database files on a SAN using Pass-Through Disk Access so that a reporting application can also access those files. In another example, a virtualized IIS 7.0 Web server might store Web content on a SAN using Pass-Through Disk Access so that a content indexing application can access those files as well.

#### New Storage Device Controller Architecture

The VMBus architecture used in Hyper-V provides a synthetic storage device controller for virtual machines. The synthetic storage device controller supports up to 255 VHDs per controller, and supports an unlimited number of controllers per virtual machine.

Guest operating systems that do not support synthetic devices will use an emulated IDE controller for storage access. The emulated SCSI controller from Microsoft Virtual Server 2005 has been removed. This is because the emulated IDE controller has been modified to surpass previous limitations. The new emulated IDE controller in Hyper-V has the same type of functionality as the emulated SCSI controller in Microsoft Virtual Server 2005.

### Robust Networking

#### VLAN Support

Windows Server virtualization makes use of virtual switches to control and secure network traffic that enters and leaves virtual machines. A Hyper-V virtual switch can be associated with a physical network Virtual LAN (VLAN) tag to limit network communication over that virtual switch to a specific VLAN. Multiple Hyper-V virtual switches can be associated with a single physical network adapter. VLAN support in Hyper-V provides increased network security for virtual machines by making it possible to restrict network communication from a virtual machine to a specific VLAN.

#### PXE Boot

Virtual network cards in Hyper-V support Pre-boot Execution Environment (PXE) startup. This network startup allows customers to provision their virtual machines in the same ways that they do their physical servers. To take advantage of this feature, the PXE infrastructure needs to be on the host network.

#### Virtual Machine NAP Support

Hyper-V can work together with the Network Access Protection (NAP) feature in Windows Server 2008 to prevent noncompliant virtual machines from accessing and compromising an organization’s network. NAP is used to configure and enforce computer health requirements and to update, or remediate, noncompliant 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 computers are noncompliant. Both client and server-side components assist in the remediation of noncompliant computers, so that the computer can obtain unlimited network access. If a computer is determined to be noncompliant, it can be denied 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.

The benefits of NAP apply to virtual machines in the same way that they apply to physical computers in the environment (more comprehensive coverage of NAP is located in Chapter 5, Security and Policy Enforcement).

### Flexible Role-based Security

Using Role-based security means limiting administrative access to one or more virtual machines on a Hyper-V running multiple virtual machines. Hyper-V uses the Windows Server 2008 Authorization Manger to assign role permissions. For example, an administrative role might be database manager for an organization’s marketing department. With a dedicated database server running in a non-virtualized configuration, the database manager can be assigned access to the database server but not any other servers in the organization.

Because non-virtualized servers are often underutilized, however, organizations are consolidating the workloads formerly deployed on dedicated servers onto consolidated servers. From the previous example, the marketing database server might be consolidated onto a server running other databases and applications. This type of consolidation makes it difficult to secure the server so that multiple administrators just the needed level of access to the required VMs without having administrative access on the host server or administrative access to other VMs. In this example, the marketing database administrator should only be able to access and manage the marketing database VM.

With Hyper-V, a workload, such as the marketing database, can be assigned its own virtual machine. Because the virtual machine presents the same security boundary as a discrete physical server, the marketing database manager can be assigned administrative access to the virtual server hosting the marketing database without giving them administrative access to the host or other virtual servers in the organization.

This capability in Hyper-V makes it possible to perform server consolidation with greater ease and flexibility.

### Hyper-V on Server Core

Hyper-V can be installed as a role on Server Core. Server Core provides an environment for running one or more of the following server roles:

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

Running Hyper-V on Server Core offers the following additional security and performance benefits:

* Reduced attack surface—Because Server Core uses a minimal set of DLLs and system components, it offers less opportunity for attack and compromise. Applications that are often targeted for attack, such as Internet Explorer, are not present in a Server Core installation of Windows Server 2008.
* Reduced software update requirements—Server Core offers a reduced set of server roles. Because a role that is not available on the server does not need to be maintained through software updates, Server Core will require smaller and less frequent Windows Update downloads. An additional benefit of Server Core is less frequent rebooting is required from Windows Updates.
* Performance—Server Core has a significantly smaller memory footprint and is the lowest-overhead platform for running Hyper-V.

Because the MMC 3.0-based management console for Hyper-V makes it easy to create and manage virtual machines from a workstation or another Windows Server 2008 server, Server Core may be the ideal Windows Server 2008 configuration for many Hyper-V installations. The WMI Provider (discussed later in this chapter) and PowerShell scripting support in Hyper-V provide powerful and flexible support for script-based management of both the host server and guest virtual machines.

Server Core installations of Windows Server 2008 can be used to host core infrastructure roles in Hyper-V virtual machines. Smaller footprint VMs based on Windows Server Core can increase VM density while enabling faster Quick Migrations, VM Snapshots, and VM backups. In addition, using Windows Server Core as the host operating system for Hyper-V can increase uptime due to the decreased patching requirements for Windows Server Core. Windows Server Core and Hyper-V are an excellent combination for highly available virtualized environments.

### Flexible Resource Control

Hyper-V is able to allocate resources among running virtual machines in a flexible, controllable manner.

#### CPU Resource Allocation

Hyper-V is able to allocate host server physical CPU resources among running virtual machines with a flexible CPU Resource Allocation model. The table below describes the settings used in Hyper-V CPU Resource Allocation calculations:

Table 3: CPU Resource Allocation Settings

|  |  |
| --- | --- |
| **Item** | **Description** |
| Relative Weight | The relative weight given to the resource needs of this virtual machine compared to all other virtual machines. A virtual machine with a higher relative weight is dynamically allocated additional resources as needed from other virtual machines that have lower relative weights. By default, all virtual machines have a relative weight of 100, so that their resource requirements are equal, and none is given preference. Administrators can assign each virtual machine a relative weight from 1 through 10,000. In most cases, this is the only setting that needs to be configured. |
| Reserved Capacity (% of one CPU) | The capacity of a single CPU that is reserved for this virtual machine. The percentage of CPU capacity that is available to it will never be less than this number. |
| Maximum Capacity (% of one CPU) | The highest percentage of the total resources of a single CPU that can be consumed by this virtual machine at any given time. |
| Reserved Capacity (% of system) | The percentage of total system CPU capacity that is reserved for this virtual machine. |
| Maximum Capacity (% of system) | The highest percentage of the total system CPU resources that can be consumed by this virtual machine at any given time. |
| Total Capacity Reserved | The total CPU capacity of the physical computer that has been reserved for all currently running virtual machines. If the physical computer has multiple CPUs, this figure represents the percent that is reserved of all CPUs combined. |
| Available Capacity Remaining | The total CPU capacity of the physical computer that has not been reserved for currently running virtual machines. If the physical computer has multiple CPUs, this figure represents the available percentage of all CPUs combined. |

Note: Hyper-V provides its own resource manager for allocating system resources to virtual machines. Other resource managers, such as Windows System Resource Manager, should not be used with Hyper-V.

### Hyper-V High Availability

Hyper-V includes enhancements that work in cooperation with Failover Clustering to ensure high availability of virtual machines running on Windows virtualization. When used in conjunction with Failover Clustering and System Center Virtual Machine Manager, Hyper-V enables administrators to respond for the need for planned downtime and react to unplanned downtime with minimum service interruption.

Hyper-V achieves highly available virtual machines using:

* Failover Clustering
* Live Migration
* Backup

#### Clustering and Hyper-V

Windows Server 2008 clustering provides a high availability for Hyper-V by allowing virtual machines to migrate to other nodes in the cluster in the event of unplanned or planned 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).

#### Host Clustering

Using Windows Server 2008 failover clustering to make the Hyper-V role highly available means that one 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 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 the running virtual machine state is managed by one of the Hyper-V nodes. In the event of planned downtime, the Quick Migration feature (discussed later in this chapter) can be used to move running virtual machines to another cluster node. In the event of unplanned downtime, the Cluster service will automatically restart virtual machines on a surviving cluster node. Host Clustering provides high availability for the entire Hyper-V platform and all virtual machines hosted on a Hyper-V server.

#### Guest Clustering

Virtual machines running in Hyper-V can be clustered, even if the underlying host operating system is not. 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, the virtual machines 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, and 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.

Network Load Balancing is a feature that distributes the load for networked client and server applications across multiple servers in an NLB cluster. NLB is particularly useful for ensuring that stateless applications, such as a Web-based applications running on Internet Information Services (IIS), 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.

#### Hyper-V and Multi-site clustering

In Windows Server 2008 failover clustering, the less than 500ms network latency requirement has been removed. The latency requirement is now configurable. In Windows Server 2008, clusters can now cross subnets. This removes a previous requirement to use a VLAN to connect cluster nodes geographically dispersed sites.

The evolution of 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.

Hyper-V Quick Migration

The Quick Migration feature of Hyper-V makes it possible to move a running virtual machine from one Hyper-V host to another. Quick Migration is supported by a Host Clustering configuration, which provides the underlying shared storage management and resource relocation technology needed for Quick Migration.

Quick Migration can be managed in three ways. First, System Center Virtual Machine Manager (SCVMM) provides a GUI interface that permits drag-and-drop migration of running virtual machines from one Hyper-V host server to another in the same cluster. If SCVMM is not in use, the Failover Clusters Manager MMC console can be used to initiate the Quick Migration of a running virtual machine from one Hyper-V host server to another in the same cluster with a minimal amount of down time. The WMI Provider in Hyper-V also makes it possible to script the Quick Migration of a running virtual machine from one Hyper-V host server to another in the same cluster. The speed of the Quick Migration is dependent upon the amount of information in memory that must be moved, and the speed of the shared storage device.

### Management Features

#### Virtual Server Migration

Microsoft Virtual Server 2005, Microsoft Virtual PC, and Hyper-V utilize the common, open VHD format for storing the file content of virtual machines. This means that existing virtual machines created in Virtual Server 2005 can be migrated to a Hyper-V host. Administrators can create and manage existing virtualized workloads in Virtual Server 2005, and after deployment, move those virtual machines directly to Hyper-V without any need to recreate the virtual machines. This ensures that administrators can continue to leverage their existing investment in a virtualized infrastructure, and gradually move that infrastructure to Hyper-V.

#### WMI Provider

Hyper-V is managed through Windows Management Instrumentation (WMI). The Hyper-V WMI Provider exposes objects that control all aspects of Hyper-V including.

* Managing server settings
* Creating and configuring virtual machines
* Creating and configuring Virtual Network switches
* Controlling the state of running virtual machines

In addition, the WMI provider allows external scripting and management tools, such as Windows PowerShell, System Center Virtual Machine Manager, and other third-party tools to manage a Hyper-V server.

#### Performance Counters

Hyper-V offers a detailed set of performance and resource utilization counters. These counters can report on resource usage on a global, or per-virtual machine, basis. These performance counters enable administrators to determine how host server resources are being used by virtual machines. This information can help administrators isolate performance problems in the Hyper-V environment and most effectively allocate Hyper-V host server hardware to virtual machines. Hyper-V utilization counters can also provide source data for chargeback accounting.

#### Critical failure notification

Hyper-V incorporates critical failure notification to recognize and respond appropriately to critical conditions. For example, a Hyper-V host server many be equipped with an Uninterruptible Power Supply (UPS). Should a power outage occur, the UPS will signal the parent partition that power has been lost and tell the parent partition how much battery life to expect. Hyper-V can respond to this critical failure notification in a variety of ways. Hyper-V can initiate one of the following responses:

* Save State and power down virtual machines
* Shut down guest operating systems
* Power off virtual machines without saving state
* Initiate a Quick Migration if the Hyper-V host is configured appropriately

#### Guest Operating System Support

Business units rely on the dynamic data center to incorporate the most effective tools for each business function, even when those tools require unique hardware or software configurations. For example, a Linux-based vertical application tied to a manufacturing process should be able to coexist with Windows-based applications in other areas.

Hyper-V supports 64-bit and 32-bit VMs running Windows, Linux, and Xen-enabled Linux, as well as 32-bit VMs compatible with most major operating systems. Servers previously dedicated to single-application functions can be replaced with VMs incorporating advanced features, such as dynamic hardware management and failover clustering.

#### Hot Backup of Running Virtual Machines

Hyper-V interacts with the Volume Shadow Copy Service (VSS) in Windows Server 2008 to permit backup of running virtual machines. This means that whole servers can be backed up, while running, in the time that it takes to copy their VHD file(s) to an alternate location.

#### Hyper-V Online Backup

Hyper-V has an integrated VSS Writer component. VSS Writers are software that is included in applications and services that help provide consistent shadow copies. When applications and services are running, the writer works with the Volume Shadow Copy Service (typically invoked through a backup program) to ensure that no writes occur on the volume while the shadow copy is being created. This allows backups to be created while VMs are online and running.

#### Hyper-V Disaster Recovery Preparation

With Hyper-V, more options are available for disaster recovery preparation compared to non-virtualized servers and compared to some other products. Because administrators can back up a running virtual machine, system backups of virtual servers can happen without downtime for the virtual server. This provides greater backup scheduling flexibility for administrators.

If a Hyper-V host server fails, all of the virtual machines on that host will be unavailable until the host server is repaired or replaced. If the administrator has backed up virtual machines from the host to an alternate location, the backed up VHD files contain all of the information needed to recover virtual machines to the point where they were backed up. If a Hyper-V server with unused hardware capacity is available, the backed up virtual machines can be restored to this alternate server, the virtual machines powered up, and service restored. Although this disaster recovery method should be tested to determine whether ancillary services are affected by this type of restore operation, it presents a compelling alternative for rapid recovery from disasters affecting a Hyper-V host.

#### Virtual Machine Snapshots

Hyper-V is integrated with the Microsoft Volume Shadow Copy service to enable administrators to create point-in-time snapshots of running virtual machines. This is useful in backup and disaster recovery scenarios. It is also useful when administrators want to implement complex or high risk configuration changes, and have the option to roll back those changes should something go wrong. When the administrator creates snapshot of a virtual machine, Hyper-V ensures that the virtual machine is in a consistent state before the snapshot is taken.

## Scenario: Consolidate Infrastructure, Application, and Remote Server Workloads

The biggest driver for adopting virtualization technology is server consolidation. Businesses are under pressure to ease management and reducecosts while retaining and enhancing competitive advantages like reliability, scalability, and security.

Hyper-V is ideal for server consolidation in the datacenter and in remote locations, enabling organizations to make more efficient use of their hardware resources. It also enables IT organizations to enhance their administrative productivity and rapidly deploy new servers to address changing business needs.

### Key Consolidation Features

Table 4: Key Consolidation Features

|  |  |
| --- | --- |
| **Feature** | **Description** |
| Broad Guest Operation System Support | Guest operating systems supported in Hyper-V include Windows Server 2008 (including Server Core), Windows Server 2003 R2 SP2, Windows Vista SP1, Windows XP Pro SP3, and SUSE Linux Enterprise Server 10. These operating systems are able to take advantage of VMBus hardware sharing and the associated performance enhancements.  In addition to supporting the operating systems above, VMs in Hyper-V emulate broadly compatible hardware, allowing many other guest operating systems to function well in Hyper-V VMs. |
| Hardware virtualization and legacy hardware emulation | VMs using supported guest operating systems interact with synthetic devices that have no real-world counterpart. Legacy operating systems interact with emulated hardware that acts like specific devices (for example, Intel 21140 network adapter). |
| P2V—Physical-to-virtual conversion | Enables physical servers to be converted to virtual machines. |
| CPU Resource Allocation | CPU resource allocationsupports both weighting and constraint methods for fine-grained control.   * Multithreaded for highly scalable performance. * Each virtual machine can use up to 100% of a single host processor core. * Multiple virtual machines can execute concurrently and make use of multiple host processor cores. * The number of virtual machines that can be hosted on any server depends on the:   + Combined processor, memory, and I/O load the virtual machines put on the host   + Processor, memory, and I/O capacity available on the host system. * Hyper-V supports both weight-based and constraint-based CPU resource allocation for balanced workload management. * The relative weight given to the resource needs of this virtual machine compared to all other virtual machines. A virtual machine with a higher relative weight is dynamically allocated additional resources as needed from other virtual machines that have lower relative weights. By default, all virtual machines have a relative weight of 100, so that their resource requirements are equal, and none is given preference. * Capacity and Weight algorithms operate concurrently:   + Contention can occur for the maximum system capacities.   + Relative weights indicate how to allocate resources during contention |
| Memory Resource Allocation | Hyper-V enables flexible memory configuration on a per-virtual machine basis, including hot-add of memory to a running VM.   * Support is included for NUMA-aware scheduling and memory allocation, reducing memory bus contention on multi-processor socket systems. * On non-NUMA systems Hyper-V relies on the Host operating system scheduler. |
| PXE Boot | Virtual network cards in Hyper-V support Pre-boot Execution Environment (PXE) boot. This network boot allows customers to provision their virtual machines in the same ways that they do their physical servers.  Note: To take advantage of this feature, the PXE infrastructure needs to be on the host network. |
| Active Directory Integration | Active Directory allows the same directory management features to be used for virtual machines as are used for physical machines, by providing a centralized repository for hierarchical information about users and computers on the network. Active Directory incorporates significant improvements in management and performance in Windows Server 2008, which can be leveraged through virtual machines hosted by Hyper-V.  Integration with Active Directory enables delegated administration and authenticated guest access. Hyper-V enables fine-grained administrative control over virtual machines with per-virtual machine ACLs that can be managed from within Active Directory’s Group Policy Management Console. Event logs are integrated with Active Directory and Microsoft Management Consoles. |

## Scenario: Automate and Consolidate Software Test and Development Environments

Hyper-V enables businesses to consolidate their test and development servers and automate the provisioning of virtual machines.

Customers across all segments are looking for ways to decrease costs and accelerate application and infrastructure installations and upgrades, while delivering comprehensive quality assurance. In order to achieve testing coverage goals prior to going into production, multiple challenges must be overcome:

* Network operations—Incorrect configuration of a test network could endanger production networks.
* Developer productivity—Developer productivity is wasted on time-consuming administrative tasks like configuring test environments and installing operating systems.
* Server operational and capital costs—High-quality application test coverage requires replicating production computing environments, which requires costly hardware and human resources posing risk to budgets and schedules.

Virtual machine technology was developed more than 30 years ago to address these same challenges first encountered during the mainframe era, enabling side-by-side testing and production partitions on the same system. Hyper-V enables better test coverage, developer productivity and user experience.

Developers can also leverage Hyper-V as an efficient tool to simulate distributed applications on a single physical server. Deployment and testing of distributed server applications typically requires quantities of available hardware resources and considerable amounts of time to configure the hardware and software systems in a lab environment to simulate a desired scenario.

Hyper-V is a powerful time and resource-saving solution that optimizes hardware and human resource utilization in distributed server application development scenarios. Hyper-V enables individual developers to easily deploy and test a distributed server application using multiple virtual machines on one physical server. Marrying the robust features in Hyper-V, like disk hierarchy and virtual networking, with the value of machine consolidation gives developers a powerful and efficient way to simulate complex network environments. The result is a development environment solution that is very time and cost effective as less hardware, less real estate, and less time are required for build-out.

Table 5: Key Software Testing and Development Features

|  |  |
| --- | --- |
| **Feature** | **Description** |
| Broad Guest operating system support | Guest operating systems supported in Hyper-V include Windows Server 2008 (including Server Core), Windows Server 2003 R2 SP2, Windows Vista SP1, Windows XP Pro SP3, and SUSE Linux Enterprise Server 10. These operating systems are able to take advantage of VMBus hardware sharing and the associated performance enhancements.  In addition to supporting the operating systems above, VMs in Hyper-V emulate broadly compatible hardware, allowing many other guest operating systems to function well in Hyper-V VMs. |
| Configuration Libraries | Hyper-V used with System Center Virtual Machine Manager includes the ability to store and manage VMs in libraries, calling them into service as needed.  Library VMs benefit from offline VHD manipulation, enabling VMs to be changed without running the associated VM. |
| Self-service Portals | System Center Virtual Machine Manager enables developers and testers to create and destroy VMs from a configuration library instead of requiring administrator intervention. |
| VM Snapshots | Snapshots enable developers and testers to roll back VM system configurations to "last known good" status.  Some kinds of development and testing involve a lot of waiting for programs and operating systems to install, uninstall, and reinstall. With the Snapshot feature of Hyper-V, a VM can be reset to a previous configuration, minimizing the need to uninstall programs or reinstall operating systems. |

## Scenario: Business Continuity and Disaster Recovery

Hyper-V can be part of a disaster recovery plan that requires application portability and flexibility across hardware platforms. Consolidating physical servers onto fewer physical machines running virtual machines decreases the number of physical assets that can be damaged or compromised in a disaster. In the event of recovery, virtual machines can be hosted anywhere, on host machines other than those affected by a disaster, speeding up recovery times and maximizing organization flexibility.

Table 6: Key Business Continuity and Disaster Recovery Features

|  |  |
| --- | --- |
| **Feature** | **Description** |
| High availability through host and guest clustering | Hyper-V enables clustering of guest operating systems and host computers, enabling a variety of high availability scenarios. Clustering host computers offers a cost-effective means of increasing server availability, enabling failover of virtual machines among the Hyper-V hosts in the cluster. Using Hyper-V organizations can create a high availability virtual machine environment that can effectively accommodate both planned and unplanned downtime scenarios without requiring the purchase of additional software tools.  For example, IT administrators can effectively anticipate server restarts if required by system updates. With a properly configured Hyper-V host cluster, running virtual machines can be migrated to another host in the cluster without downtime.  In unplanned downtime scenarios, such as hardware failure, the virtual machines running on the host can be automatically migrated to the next available Hyper-V host.  Guest clustering allows cluster-aware applications to be clustered within virtual machines across Hypver-V host computers. |
| Live Backup | Hyper-V includes the ability to back up running virtual machines and their data without downtime. If a server goes down, its VMs can be restored and started on any other server, minimizing service interruptions.  Tape backup processes take advantage of virtual tape drive functionality in Hyper-V. If a server incorporates a script to automatically back up its data to a tape drive, for example, that process can still be used when the server is converted to a virtual machine. |
| Health Monitoring | Hyper-V leverages comprehensive integration with monitoring tools like System Center Operations Manager to spot and respond to issues before they become larger problems. |

## Scenario: Enabling the Dynamic Datacenter

Data centers face increased pressure to optimize hardware and facilities usage while increasing performance and leveraging business intelligence. Hyper-V gives data centers the agility to respond to changing needs and the power and flexibility to design for the future.

Core features like 64-bit, multi-processor support, and flexible resource control enable data centers to rely on virtual machines for even the most resource-intensive workloads.

Hyper-V helps realize the dynamic data center vision of providing self-managing dynamic systems and operational agility. Combining business processes with System Center Virtual Machine Manager enables a datacenter to leverage rapid provisioning of new applications and dynamic load balancing of virtual workloads across different physical machines in their infrastructure and progress toward self-managing dynamic systems.

### MSC Integration

Hyper-V integrates with Microsoft System Center (MSC), a new generation of dynamic management tools designed to support the Dynamic Systems Initiative (DSI). MSC provides IT Professionals with the tools and knowledge to help manage their IT infrastructure, embedding operational knowledge in the management tools and enabling the system to manage and even heal itself.

The essence of Microsoft's DSI strategy is to develop and deliver technologies that enable businesses and the people in them to be more productive and to better adapt to dynamic business demands. There are three architectural elements of the dynamic systems technology strategy:

1. Design for Operations to capture the diverse knowledge of people, such as business architects, application developers, IT Professionals, and industry partners, by embedding it within the IT infrastructure itself through the use of system models.
2. Knowledge-driven management that enables systems to capture desired states of configuration and health in models and uses this inherent knowledge to provide a level of self-management to systems.
3. Virtualized Infrastructure to achieve greater agility and leverage existing infrastructure by consolidating system resources into a virtual service pool. Virtualized infrastructure makes it is easier for a system to quickly add, subtract, move, or change the resources it draws upon to do its work, based on business priorities and demands.

These three elements are the foundation for building dynamic systems. Virtualized infrastructure mobilizes the resources of the infrastructure, Knowledge-Driven Management is the mechanism for putting those resources to work to meet dynamic business demands, and Design for Operations ensures systems are built with operational excellence in mind.

For more information about DSI, see: http://www.microsoft.com/dsi/.

Table 7: Key Dynamic Datacenter Features

|  |  |
| --- | --- |
| **Feature** | **Description** |
| Broad Guest OS support | Guest operating systems supported in Hyper-V include Windows Server 2008 (including Server Core), Windows Server 2003 R2 SP2, Windows Vista SP1, Windows XP Pro SP3, and SUSE Linux Enterprise Server 10. These operating systems are able to take advantage of VMBus hardware sharing and the associated performance enhancements.  In addition to supporting the operating systems above, VMs in Hyper-V emulate broadly compatible hardware, allowing many other guest operating systems to function well in Hyper-V VMs. |
| Utilization Counters | Hyper-V utilization counters enable datacenters to obtain virtual server utilization information to facilitate capacity planning decisions. |

## Virtualization Beyond the Server

Hyper-V is a component of a complete virtualization solution that includes every stage from the desktop to the datacenter.

* Desktop virtualization with Microsoft Virtual PC 2007 enables users to run guest operating systems. It is commonly used for testing vertical applications during development that require different operating systems. In additional, a trainer might distribute Virtual PC files to all students in a class to make sure they are all working on identical setups.
* Application virtualization with Microsoft SoftGrid® Application Virtualization insulates applications running on the same operating system, helping to eliminate potential conflicts and enable rapid provisioning. An application that would usually update the registry, for example, updates a virtual registry, so the system is able to meet the application's requirements without impacting other applications. Applications can be installed and uninstalled more quickly than through typical setup and uninstall procedures, including custom options that would otherwise have to be configured manually.
* Presentation virtualization through Microsoft Terminal Services enables remote users to access applications and operating systems hosted from remote locations. A common usage model is accessing the office desktop computer or server-based applications from home or while traveling, giving the remote user the ability to manipulate local files, log into applications that require access to hardware on the desktop computer, and use other resources that wouldn't otherwise be available remotely. Presentation virtualization has the added benefit of enabling resource-intensive applications to be used through lower-power laptops or other computers that would otherwise be incompatible, even ones running different operating systems. Presentation Virtualization will be covered in detail in the next chapter of this paper.

## Summary

Hyper-V is a cost-effective and well-supported server virtualization technology for the Windows Server 2008 platform. The move Microsoft has made to hypervisor-based, hardware-assisted virtualization vastly improves reliability and scalability for virtual servers, enabling even the most demanding workloads to be run in dynamic virtual machines. Hyper-V's industry-standard management tools enable system administrators to manage virtual servers and physical servers in the same familiar, widely supported interface.

Hyper-V allows organizations to consolidate infrastructure, application, and branch office server workloads. Hyper-V is ideal for server consolidation in both the datacenter and remote locations, allowing organizations to make more efficient use of their hardware resources. It also allows IT organizations to enhance their administrative productivity and rapidly deploy new servers to address changing business needs. Hyper-V enables businesses to consolidate their test and development server farm and automate the provisioning of virtual machines. Hyper-V can also be used as part of a disaster recovery plan that requires application portability and flexibility across hardware platforms. Finally, Hyper-V gives data centers the agility to respond to changing needs and the power and flexibility to design for the future.

# Chapter 3: Presentation Virtualization with TS RemoteApp

## Introduction

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

Windows Server 2008 adds improvements and innovations to Terminal Services that facilitate allow organizations to provide remote users with easy access to applications using a Web browser, as well as providing a means to access remote terminals and applications across firewalls. This mitigates deployment costs, and helps ensure a consistent application experience and performance regardless of the user’s location.

## Terminal Services RemoteApp

Terminal Services provides technologies that enable access, from almost any location, to a server running Windows-based programs or the full Windows desktop. Users can connect to a terminal server to run programs and use network resources on that server. With TS applications and data live in the datacenter, and only encrypted keyboard and mouse strokes are transmitted over the network.

Terminal Services RemoteApp is the new remote application presentation method included in Windows Server 2008. RemoteApp complements the Terminal Services presentation method, which presents the entire remote desktop to users who access applications within that window.

With TS RemoteApp, the user’s interaction with remote applications is significantly different. Now the remote application, not the entire remote desktop, launches, and runs in its own resizable window on the client computer’s desktop. 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 even be unaware that the remote program is any different than other local applications running side-by-side with the remote program on their desktop.

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

For a program to run remotely using Remote Programs, the terminal server hosting the program must be running Windows Server 2008 and Remote Desktop Connection 6.0 (or later). Any program that can run in a Terminal Services session or in a Remote Desktop session can run as a Remote Program.

## Terminal Services

Terminal Services includes new core functionality that enhances the end-user experience when connecting to a Windows Server 2008 terminal server. This new core functionality includes:

* Remote Desktop Connection 6.0 or later
* Remote Desktop Connection display improvements, including:
  + Custom display resolutions
  + Monitor spanning
  + Desktop experience
  + Desktop composition
  + Font smoothing
  + Display data prioritization
* Plug and Play device redirection for media players and digital cameras
* Windows Embedded for Point of Service device redirection
* Single Sign-On
* TS Session Broker
* TS Easy Print
* Licensing Improvements

### Remote Desktop Connection 6.0 and later

To access Terminal Services, users will need to use the Remote Desktop Connection 6.0 or later. It is included with both Windows Server 2008 and Windows Vista, and is available as free a download for Windows XP users and Windows Server 2003.

#### Remote Desktop Connection display

The Remote Desktop Connection 6.0 or later software adds support for using higher-resolution desktop computers. The Desktop Experience feature and the display data prioritization settings are designed to enhance the end-user experience when connecting remotely to a Windows Server 2008 terminal server.

Custom display resolution provides support for additional display resolution ratios, such as 16:9 or 16:10 wide screen formats. For example, newer monitors with resolutions of 1680 x 1050 or 1920 x 1200 are now supported. The maximum resolution supported is 4096 x 2048.

#### Monitor Spanning

The Remote Desktop Connection also supports monitor spanning, which allows the user to display the remote desktop session across multiple monitors.

The monitors used for monitor spanning must meet the following requirements:

* All monitors must use the same resolution. For example, two monitors using 1024 x 768 resolution can be spanned. But one monitor at 1024 x 768 and one monitor at 800 x 600 cannot be spanned.
* All monitors must be aligned horizontally (that is, side by side). There is currently no support for spanning multiple monitors vertically on the client system.
* The total resolution across all monitors cannot exceed 4096 x 2048.

#### Desktop Experience

Remote Desktop Connection 6.0 or later reproduces the desktop that exists on the remote computer on the user’s client computer. With Desktop Experience installed on the Windows Server 2008, the user can use Windows Vista features, such as Windows Media® Player, desktop themes, and photo management within their remote connection. The Desktop Experience feature and the display data prioritization settings—designed to keep the keyboard and mouse in sync with what is displaying on the monitor even under heavy bandwidth usage—enhance the end user experience when connecting to a Windows Server 2008 terminal server.

Windows Vista provides a visually dynamic experience called Windows® Aero™. Windows Aero provides features such as:

* Translucent windows
* Taskbar buttons with thumbnail-sized window previews
* A view of the open windows in a three-dimensional stack on the desktop

A Windows Server 2008 terminal server can be configured to provide Windows Aero features when a Windows Vista client computer connects to the Windows Server 2008 terminal server by using Remote Desktop Connection. This functionality is referred to as desktop composition.

For the Windows Vista client computer to use desktop composition in a remote desktop connection to a Windows Server 2008 terminal server, the Windows Vista client computer must have hardware installed that is capable of supporting Windows Aero. The Windows Server 2008 terminal server, however, does not need to have a hardware configuration that supports Windows Aero.

#### Display data prioritization

Display data prioritization automatically controls virtual channel traffic so that display, keyboard, and mouse data is given a higher priority over other virtual channel traffic, such as printing or file transfers. This prioritization is designed to ensure that screen performance is not adversely affected by bandwidth intensive actions, such as large print jobs.

The default bandwidth ratio is 70:30. Display and input data will be allocated 70 percent of the bandwidth, and all other traffic, such as clipboard, file transfers, or print jobs, will be allocated 30 percent of the bandwidth. The display data prioritization settings can be adjusted by making changes to the registry of the terminal server.

#### Font Smoothing

Windows Server 2008 supports ClearType, which is a technology for displaying computer fonts so that they appear clear and smooth, especially when using an LCD monitor.

A Windows Server 2008 terminal server can be configured to provide ClearType functionality when a client computer connects to the Windows Server 2008 terminal server by using Remote Desktop Connection. This functionality is referred to as font smoothing. Font smoothing is available if the client computer is running any of the following:

* Windows Vista
* Microsoft Windows Server 2003 with Service Pack 1 and the Remote Desktop Connection 6.0 or later software
* Windows XP with Service Pack 2 and the Remote Desktop Connection 6.0 or later software

Font smoothing allows the local settings on the client computer to help determine the user experience in the remote desktop connection. Allowing font smoothing does not change the display settings on the Windows Server 2008 terminal server.

Using font smoothing in a remote desktop connection will increase the amount of bandwidth used between the client computer and the Windows Server 2008 terminal server.

### Plug and Play Device redirection

In Windows Server 2008, the ability to redirect client-side devices over Terminal Services connections is enhanced and expanded. Users can now redirect Windows Portable Devices, specifically media players based on the Media Transfer Protocol (MTP), and digital cameras based on the Picture Transfer Protocol (PTP). The support for redirection supports Plug and Play devices. The Remote Desktop Protocol (.rdp) file created by the Remote Programs Wizards automatically enables Plug and Play device redirection.

When the session to the terminal server is launched, the Plug and Play device that is redirected will get automatically installed on the client computer. Plug and Play notifications will appear in the taskbar on the client computer. Redirection of Plug and Play devices is available only in Windows Vista Enterprise and Windows Vista Ultimate when connecting to a remote computer running Windows Vista.

After the redirected Plug and Play device is installed on the client computer, the Plug and Play device is available for use in the session. For example, if a Windows Portable Device such as a digital camera is redirected, the device can be accessed directly from an application, such as the Scanner and Camera Wizard on the remote computer.

Plug and Play device redirection is not supported over cascaded terminal server connections. For example, if a Plug and Play device is attached to the local client computer, it can be redirected and used when the client is connected to a terminal server (Server1, for example). If from within that remote session on Server1, the user then connects to another terminal server (Server2, for example), they will not be able to redirect and use the Plug and Play device in that remote session with Server2.

### Windows Embedded for Point of Service device redirection

Windows Server 2008 also supports redirection of Windows Embedded for Point-of-Service (POS) devices that use Microsoft POS for .NET 1.1. Examples of Windows Embedded for Point of Service (POS) devices include full-function point-of-sale workstations, network bootable “thin client” point-of-sale terminals, customer-facing information kiosks and self-checkout systems. However, Windows Embedded for POS device redirection is only supported if the terminal server is running a 32-bit version of Windows Server 2008.

By default, Microsoft POS for .NET devices are not found on the client computer, in **Remote Desktop Connection**, on theLocal Resourcestab, listed under Local devices and resources. Therefore, to enable Microsoft POS for .NET devices for redirection, the Remote Desktop Protocol (.rdp) used to connect to the terminal server must be edited. The following line must be changed or added: redirectposdevices:i:<value>

* If <value> =0, Microsoft POS for .NET device redirection is disabled.
* If <value> =1, Microsoft POS for .NET device redirection is enabled.

Note: The .rdp file created by the Remote Programs Wizard automatically enables Microsoft POS for .NET device redirection.

After Microsoft POS for .NET 1.1 has been configured on the terminal server and Windows Embedded for POS device redirection has been enabled in the .rdp file on the client computer, Windows Embedded for point of sale (POS) devices can be plugged in to the client computer. The client computer can then connect to the terminal server using the modified .rdp file. When the user connects the Windows Embedded for POS device will be automatically installed on the Terminal Server. Plug and Play notifications will appear as well.

After the redirected Windows Embedded for POS device is installed on the Terminal Server, the Windows Embedded for POS application residing on the terminal server can access the Windows Embedded for POS physically connected to the client computer.

### Single Sign-On (SSO)

Single Sign-On (SSO) allows users with a domain account to log on to a Terminal Services session once, using a password or smart card, and then gain access to remote servers without being asked for their credentials again.

Line of Business (LOB) applications deployment and centralized application deployment are key scenarios for using single sign-on. Due to lower maintenance costs, many companies prefer to install their LOB applications on a terminal server and make these applications available through Terminal Services Remote Programs or Remote Desktop. Single sign-on makes it possible to give users a better experience by eliminating the need for users to enter credentials every time they initiate a remote session.

Single sign-on for remote connections can only be used from a Windows Vista-based computer connecting to a Windows Server 2008 terminal server or from one Windows Server 2008 server connecting to another. The user accounts that are used for logging on must have appropriate rights to log on to both the terminal server and the Windows Vista client and both the client computer and terminal server must be joined to a domain.

### TS Session Broker

TS Session Broker is a new feature in Windows Server 2008 that provides an easier alternative to Microsoft Network Load Balancing for Terminal Services. While not limited to a specific number of servers, the feature provides significant value to farms of two to five servers. With TS Session Broker, new sessions are distributed to the least loaded server within the farm. This optimizes performance while allowing users to reconnect to an existing session without having to know specific information about the server where their session was established. IT managers can use the feature to map the Internet Protocol (IP) address of each Terminal Server to a single Domain Name System (DNS) entry. This configuration can also provide fault tolerance; in the event one of the farm servers is unavailable the user will connect to the next least loaded server in the farm.

### Printing Enhancements

Windows Server 2008 provides performance and scalability enhancements to Terminal Services printing. Improvements include redirected printers getting installed on remote sessions much more quickly, and a single Windows Server 2008 terminal server handling a larger number of redirected client printers.

### TS Easy Print

TS Easy Print is a new feature in Windows Server 2008 that enables users to reliably print from a TS RemoteApp or full desktop session to a local or network printer installed on the client computer. Printers can now be supported without the need to install print drivers on the terminal server. When a user wants to print from a TS RemoteApp program or desktop session, they will see the full printer properties dialog box (printer user interface) from the local client and have access to all the printer functionality. IT administrators can use Group Policy to limit the number of printers redirected to just the default printer, rather than allowing multiple printers to be redirected, thereby reducing overhead and improving scalability.

### Licensing Improvements

Terminal Server Licensing is the client license management service for Terminal Service clients in the Windows Server 2008. The Terminal Server Licensing service works with Terminal Server to provide, catalog, and enforce license policy among Terminal Server clients.

Terminal Services Licensing in Windows Server 2008 has new features that enable better deployment and management of Licensing environments including per-user tracking and reporting, manual revocation of licenses, better diagnostics and support for WMI providers.

New or enhanced features include:

* Terminal Services Per-Device client access license—Terminal Services Licensing (TS Licensing) now allows a Terminal Services Per-Device client access license (TS Per-Device CAL) which permits one device (used by any user) to conduct Windows sessions on any of an organization’s servers.
* Terminal Services Per-User client access license—Terminal Services Per-User client access license (TS Per-User CAL) permits one user (using any device) to conduct Windows sessions on any of an organization’s servers.

TS Licensing for Windows Server 2008 now includes the ability to track the issuance of TS Per-User CALs by using the TS Licensing management tool. If the terminal server is in Per-User licensing mode, the user connecting to it must have a TS Per-User CAL. If the user does not have the required TS Per-User CAL, the terminal server will contact the license server to get the CAL for the user. After the license server issues a TS Per-User CAL to the user, the administrator can track the issuance of the CAL by using the TS Licensing management tool. IT staff can also use Windows Management Instrumentation (WMI) scripts to generate license tracking reports on the command line.

#### Terminal Services License server (TS Licensing)

Windows Server 2008 also uses a Terminal Services license server. A Terminal Services license server is a computer on which the TS Licensing role service is installed. A license server stores all TS CAL tokens that have been installed for a group of terminal servers and tracks the license tokens that have been issued. One license server can serve many terminal servers simultaneously. To issue permanent license tokens to client devices, a terminal server must be able to connect to an activated license server. A license server that has been installed but not activated will only issue temporary license tokens.

In Windows Server 2008, there are two types of license servers (formerly roles). These servers are:

* Domain license server
* Forest license server (formerly "Enterprise")

To take advantage of TS Licensing, organizations must meet these prerequisites:

* IT staff must install the TS Licensing role service on a server running Windows Server 2008.
* TS Per-User CAL tracking and reporting is supported only in domain-joined scenarios (the terminal server and the license server are members of a domain) and is not supported in workgroup mode. Active Directory® Domain Services is used for license tracking in Per-User mode. Active Directory Domain Services can be Windows Server 2008-based or Windows Server 2003-based. *Note*: No updates to the Active Directory Domain Services schema are needed to implement TS Per-User CAL tracking and reporting.
* A terminal server running Windows Server 2008 does not communicate with a license server running Windows Server 2003. However, it is possible for a terminal server running Windows Server 2003 to communicate with a license server running Windows Server 2008.

#### Per-User Tracking and Reporting

Prior to Windows Server 2008, per-user licenses were not issued. There was no easy way to track if the usage of per-user licenses was in line with the End-User License Agreement (EULA) or other licensing agreements. With Windows Server 2008, IT groups can easily track usage and create reports of how many per-user licenses were issued. Reports can be accessed both through the License Manager UI as well as the WMI providers.

*Note*: Per-user licenses are only tracked and not enforced.

#### Revoking a License

Some customers wanted to have the ability to revoke a license and make it available immediately to be used elsewhere. Previously, it was not possible to revoke a license issued to a client; issued licenses would automatically expire after a random period between 52-89 days, and become part of the available license pool. Windows Server 2008 now has support for revoking a license to make it available immediately\*. Through the License Manager UI or the new WMI providers in Windows Server 2008, IT professionals can select a per-device CAL that was issued to a particular client machine and choose to revoke it.

\**Note*: Only 20% of a specific version of a CAL can be revoked at a time.

## Terminal Services Gateway (TS Gateway)

Terminal Services Gateway (TS Gateway) is a Terminal Services role that allows authorized remote users to connect through the Internet to terminal servers and workstations on a corporate network. This enables organizations to make selected servers and workstations easily and securely available to remote or traveling workers without using a VPN connection.

Some of the key benefits of TS Gateway:

* Enables remote users to connect securely to resources on the corporate network from the Internet, without the complexity of Virtual Private Network (VPN) connections. Provides a more secure model, allowing users to access only selected servers and workstations instead of the entire corporate network through a VPN.
* 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).
* TS Gateway transmits all RDP traffic (that typically would have been sent over port 3389) to port 443, by using an HTTP Secure Sockets Layer (SSL) tunnel. This means that all traffic between the user's client computer and TS Gateway is encrypted while in transit over the Internet.

### TS Gateway Management

The TS Gateway Management snap-in console enables administrators to configure policies that must be met for users to connect to resources on the network. The TS Gateway Management snap-in console provides tools to help administrators monitor TS Gateway events. By using TS Gateway Management, users can specify events, such as unsuccessful connection attempts to the TS Gateway server that they want to monitor. When these events occur, the corresponding events can be monitored using the Event Viewer.

TS Gateway Management also enables the IT staff to view details about active user connections, set maximum connection limits, and perform other actions to control access to network resources through a TS Gateway server.

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.

### TS Gateway Functionality

TS Gateway in Windows Server 2008 provides several new features to simplify administration and enhance security.

#### Connection Authorization Policies (CAPs)

Connection authorization policies (CAPs) allow administrators to specify users, user groups, and optionally, computer groups that can access a TS Gateway server. TS Gateway Management creates CAPs. CAPs simplify administration and enhance security by providing a greater level of control over access to remote computers on the corporate network.

Using CAPs, administrators can require that users, user groups, or computer groups meet specific conditions to access a TS Gateway server. Specific conditions can be listed for each CAP. For example, administrators can specify connection requirements such as the use of a smart card, may define specific user groups that are allowed to connect to resources on the corporate network, may define specific resources to which users can connect, may define specific user group membership requirements, and so forth. A user is granted access to a TS Gateway server only if he or she meets or exceeds the conditions specified in the CAP that contains their group name.

#### Resource groups and Resource Authorization Policies (RAPs)

After CAPs are defined, resource groups must be created and Resource Authorization Policies (RAPs) defined that allow users access from the TS Gateway server to specific remote computers on the network. CAPs and RAPs are created and managed by using TS Gateway Management console.

Resource groups enable administrators to define the groups of remote computers that users can access. RAPs enable the management of user access to resource groups. Users connecting to the network through a TS Gateway server are granted access to specific remote computers on the network, only if they meet or exceed the conditions specified in at least one RAP. Instead of creating a resource group manually, a security group can be defined in Active Directory directory service, and is used to manage access conditions.

To ensure that the right users have access to the correct remote computers on the network, administrators must plan and create resource groups carefully. Evaluation is required to determine which users should have access to each resource group, and then one or more RAPs must be created to grant the users access as needed.

#### Monitoring capabilities

TS Gateway Management provides the ability to view information about active connections from clients to remote computers on the network through TS Gateway. This information includes the IP address of the client, the name of the user logged on to the client, the name of the remote computer to which the client is connected, and the length of time that the connection is idle, if applicable. Administrators can also specify events that they want to monitor, and then monitor these events by using Event Viewer.

#### Integration with Network Web Access Protection (NAP)

TS Gateway integrates with Network Access Protection (NAP) to enhance security in Windows Server 2008. IT Professionals can configure TS Gateway servers and clients to use NAP. In such a scenario, a remote user attempting to access a terminal server with a computer that did not meet network security requirements would be denied access to the terminal server by means of TS Gateway.

NAP is a health policy creation, enforcement, and remediation technology that is included in Windows Vista and Windows Server 2008. With NAP, system administrators can enforce health requirements on Terminal Services clients that connect to the TS Gateway server. By using NAP, IT staff can help ensure that Terminal Services clients meet the health policy requirements of the organization before those clients are allowed to connect to computers on the corporate network through TS Gateway servers (for more information about NAP, see Chapter 5: Security and Policy Enforcement).

*Note*: NAP technology does not apply to TS terminals.

## Terminal Services Web Access

Terminal Services Web Access (TS Web Access) is a Terminal Services role that lets administrators make Terminal Services RemoteApp programs available to users from a Web browser without requiring any software installation by the user. With TS Web Access, users can visit 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 a centralized menu showing all remote applications that are currently available; and running a remote application is as simple as choosing a program from the menu.

After TS Web access has been installed on a Windows Server 2008 Web server, users can connect to the TS Web Access server to access Remote Programs that are available on one more Windows Server 2008-based terminal servers. Benefits of TS Web Access include:

* Users can access Remote Programs from a Web site over the Internet or from an intranet. To start a remote program, the user just clicks the program icon.
* Using Remote Programs, a program appears as it does when running on the local computer.
* If a user starts more than one remote program and the programs are running on the same terminal server, the programs run within the same Terminal Services session.
* By using TS Web Access, there is much less administrative overhead. Programs can be easily deployed from a central location. Because programs are running on a terminal server and not on the client computer, servers are easier to maintain.
* TS Web Access provides a solution that works with minimal configuration. The TS Web Access Web page includes a customizable Web Part, which can be incorporated into a customized Web page or a Windows SharePoint® Services site.
* The list of available programs that appears in the Terminal Services Remote Programs Web Part can be customized to the individual user if Remote Programs are deployed by using Group Policy software distribution.
* TS Web Access can also be used to provide access to a full desktop.

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

### Improved Web experience

TS Web Access provides a much improved Web experience over earlier versions of Terminal Services. These improvements include:

* With TS Web Access, a user does not have to start the Remote Desktop Connection (RDC) client to start a Remote Program. Instead, he or she can access a Web page, and then click a program icon.
* The Remote Programs look as if they are running on the local desktop.
* If the user starts multiple programs and the programs are all running on the same terminal server, the programs run in the same Terminal Services session.
* Users do not have to download a separate ActiveX® control to access TS Web Access. Instead, RDP client version 6.0 or later includes the required ActiveX control.

### TS Remote Programs List is dynamically updated

When TS Web Access deploys, the list of Remote Programs that appears in the Terminal Services Remote Programs Web Part is dynamically updated. The list is populated from either the Allow List of a single terminal server.

An administrator can specify the data source that will be used to populate the list of Remote Programs. When the data source is a single terminal server, the Web Part is populated with all Remote Programs that are configured for Web access on that server's Allow List. The list of programs displayed in the Web Part is not specific to the current user.

The dynamically updated program list and the ability to specify the Remote Programs data source simplifies the deployment of Remote Programs over the Web. If there is only a single terminal server, it is easy to deploy programs by using the Terminal Server data source. Earlier versions of Terminal Services did not provide a mechanism to dynamically update a Web site with a list of remote programs.

### The Terminal Services Remote Programs Web Part

TS Web Access provides a customizable Terminal Services Remote Programs Web Part, where the list of Remote Programs is displayed. The Web Part can by deployed by using either of the following methods:

* Deploy the Remote Programs Web Part as part of the TS Web Access Web page. (This is the default out-of-the-box solution.)
* Deploy the Web Part as part of a customized Web page.

TS Web Access provides a flexible out-of-the-box solution. The provided TS Web Access Web page and Web Part allows the implementation of the TS Web Access site quickly and easily, and lets users deploy TS Web Access by using a Web page.

## Summary

With Terminal Services in Windows Server 2008, Microsoft released its most powerful presentation virtualization platform ever. Terminal Services offer a wide array of new capabilities that dramatically improve the administrator and user experiences of applications deployed and managed by using Terminal Services. Windows Server 2008 improves Terminal Services by providing a security-enhanced, easy-to-manage platform for delivering “anywhere access” to centrally managed applications and resources.

Presentation virtualization with TS RemoteApp simplifies remote connectivity, enabling rich applications to be accessed from a Web page and seamlessly integrated with the local desktop, improving remote worker efficiency. Terminal Services presentation virtualization helps organizations keep critical intellectual property secure. It also simplifies regulatory compliance by removing applications and data from the desktop.

# Chapter 4: Remote Locations

## Introduction

Businesses want to get closer to their customers, and are moving workers away from central locations, to remote locations like branch offices. With the growing number of remote locations, the IT management needs and security concerns for these locations is also growing. 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 on-site, servers in these sites 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 off site, server solutions that provide centralized management, as well as remote administration and deployment, are preferred.

Microsoft began addressing these challenges in Microsoft Windows Server 2003 R2. 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, the key benefits provided by Windows Server 2008 can be divided into three categories:

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

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 key 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 on-going challenge for IT Professionals. Windows Server 2008 simplifies remote deployment and on-going administration of the servers located in branch offices. Many of the new features and enhancements directly address the needs and concerns of the branch office, including:

* Enhanced manageability of Active Directory
* Introduction of the Read-Only Domain Controller (RODC)
* BitLocker
* Role Separation
* Server Core

### 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 remote locations. Some key management enhancements include:

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

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.

### Read-Only Domain Controllers (RODC)

A read-only domain controller (RODC) is a new type of domain controller available in the Windows Server 2008 operating system. An RODC provides a way to deploy a domain controller more securely in branch office locations that require fast, reliable and robust authentication services.

RODC is designed primarily to be deployed in remote locations and branch office environments. Remote sites typically have relatively few users, may have less physical security, relatively poor network bandwidth to a hub site, and little local IT knowledge. Inadequate physical security is the most common reason to consider deploying an RODC. However, an organization might choose to deploy an RODC for special administrative requirements.

Remote locations pose challenges for network administrators who must provide Active Directory domain services to users connected over lower speed WAN links. Having no local domain controller might delay logging on, processing group policies, and accessing network services because of the limitations of the WAN link. On the other hand, deploying and maintaining a domain controller at a remote location could be challenging if there is no local IT staff on site to support it and where physical security of the server cannot be guaranteed. The RODC addresses these problems with the following functionality:

* Read-only Active Directory database
* Unidirectional replication
* Credential caching
* Administrator role separation
* New MMC snap-in functions

#### Read-only Active Directory database

Except for account passwords, an RODC holds all of the Active Directory objects and attributes that a writable domain controller holds. However, changes cannot be made to the replica that is stored on the RODC. This prevents a change that could otherwise be made at branch locations from corrupting the forest. Local applications that request Read access to the directory can obtain access. Lightweight Directory Application Protocol (LDAP) applications that request Write access receive an LDAP referral response which directs them to a writable domain controller, which is usually in a hub site.

#### Unidirectional replication

Because no changes are written directly to the RODC, no changes originate at the RODC. Accordingly, 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, and the effort required to monitor replication. RODC unidirectional replication applies to both AD DS and Distributed File System (DFS) Replication. The RODC performs normal inbound replication for AD DS and DFS Replication changes. With branch offices relying on WAN links to connect to the central servers, this is another way that Windows Server 2008 helps optimize bandwidth usage between remote locations and hub sites.

#### Credential caching

Credential caching is the storage of user or computer credentials. Credentials are a small set of passwords that are associated with security principals (user and computer accounts). By default, an RODC does not store user or computer credentials. The exceptions are the computer account of the RODC, and a special Kerberos Ticket-Granting Ticket (*krbtgt)* account that each RODC has. The administrator must explicitly allow any other credential caching on an RODC.

The RODC is advertised as the Key Distribution Center (KDC) for the branch office. The RODC uses a different krbtgt account and password than the KDC does on a writable domain controller than when it signs or encrypts Ticket-Granting Ticket (TGT) requests.

After an account is successfully authenticated, the RODC attempts to contact a writable domain controller at the hub site, and requests a copy of the needed credentials. The writable domain controller recognizes that the request is coming from an RODC and consults the Password Replication Policy in effect for that RODC.

The Password Replication Policy determines whether a user's or computer's credentials can be replicated from the writable domain controller to the RODC. If the Password Replication Policy allows it, the writable domain controller replicates the credentials to the RODC, where they are cached.

After the credentials are cached on the RODC, the RODC can directly service that user's logon requests until the credentials change. When a TGT is signed with the krbtgt account of the RODC, the RODC recognizes that it has a cached copy of the credentials. If another domain controller has signed the TGT, the RODC will forward requests to a writable domain controller.

By limiting credential caching only to users who have authenticated to the RODC, the potential exposure of credentials by a compromise of the RODC is also limited. This is because typically only a small subset of domain users has credentials cached on any given RODC. If the RODC is compromised, only those credentials that are cached can potentially be compromised.

Leaving credential caching disabled might further limit exposure, but would result in all authentication requests being forwarded to a writable domain controller, often connected by a slower speed WAN link. An administrator can modify the default Password Replication Policy to allow users' credentials to be cached at the RODC.

When an RODC is deployed, the Password Replication Policy that will be its replication partner must be configured on the writable domain controller. The Password Replication Policy acts as an access control list (ACL). It determines if an RODC should be permitted to cache a password. After the RODC receives an authenticated user or computer logon request, it refers to the Password Replication Policy to determine if the password for the account should be cached. Subsequent logons by the same account can then be performed more efficiently.

The Password Replication Policy lists the accounts that are permitted to be cached, and accounts that are explicitly denied from being cached. The list of user and computer accounts that are permitted to be cached does not imply that the RODC has necessarily cached the passwords for those accounts. For example, an administrator can specify in advance any accounts that an RODC will need to cache. This way, the RODC can authenticate those accounts (once their credentials have been cached), even if the WAN link to the hub site is offline.

#### Administrator role separation

The local administrator role of an RODC can be delegated to any domain user without granting that user any user rights for the domain or other domain controllers. This permits a local branch user to log on to an RODC and perform maintenance work on the server, such as upgrading a driver. However, the user in the branch office cannot log on to any other domain controller or perform any other administrative tasks in the domain. In this way, the user in the branch office can be delegated the ability to effectively manage the RODC in the branch office without compromising the security of the rest of the domain. Administration role separation provides a flexible administration model while enhancing security, especially in branch offices where some local control or maintenance may be needed but the central network and servers must be protected.

#### New MMC snap-in functions

The Active Directory Sites and Services snap-in in Windows Server 2008 includes a Find command on the toolbar and on the Actionmenu. This command helps to find the site in which a domain controller is placed; this can help with troubleshooting replication problems between domain controllers in branches and hubs.

To help manage RODCs, there is now a Password Replication Policy tab on the domain controller Properties sheet. An administrator can click theAdvanced button on this tab to see what:

* passwords have been sent to the RODC
* passwords are currently stored on the RODC
* accounts have authenticated to the RODC, including accounts that are not currently defined in the security groups that are allowed or denied replication—the administrator can see who is using the RODC and can determine whether to allow or deny password replication

### Read-only Domain Name System

The Domain Name System (DNS) Server service can be installed on an RODC. An RODC is able to replicate all application directory partitions that DNS uses, including ForestDNSZones and DomainDNSZones. If the DNS server is installed on an RODC, clients can query it for name resolution as they would query any other DNS server. This allows branch clients to resolve names on their local, high-speed LAN, without having to send name resolution requests over lower-speed WAN links.

The DNS server on an RODC, however, does not support client updates directly. Consequently, the RODC does not register name server (NS) resource records for any Active Directory-integrated zone that it hosts. When a client attempts to update its DNS records against an RODC, the server returns a referral to a writeable domain controller. The client can then attempt the update the DNS server provided in the referral. In the background, the DNS server on the RODC will attempt to replicate the updated record from the DNS server that made the update. This replication request is only for a single object—the DNS record. The entire list of changed zone or domain data does not get replicated during this special replicate-single-object request.

### Server Virtualization with Hyper-V

Hyper-V, the Windows Server 2008 virtualization solution, enables organizations to consolidate servers and reduce the cost of server ownership by maximizing hardware utilization, consolidating workloads and reducing management costs. Hyper-V can consolidate servers running applications and services in the remote infrastructure onto fewer, or even a single physical server, while at the same time maintaining the isolation of the different operating system environments. The virtualized servers can be managed remotely from the central hub site using the same management interfaces already familiar to IT Professionals. More comprehensive coverage of Virtualization can be found in Chapter 2, Server Virtualization with Hyper-V.

## Remote Management and Security Enhancements

Windows Server 2008 provides a variety of new features and enhancements that offer improved security and better remote management for the IT Professional responsible for managing servers in remote locations.

### Introduction to 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 common infrastructure roles which are commonly deployed in remote locations like branch offices. Windows Server 2008 enables administrators to reduce security risks and simplify management of remote servers by using a Server Core installation to provide just the specific functionality needed on remote office servers. Server Core is covered in detail in the Server Management chapter of this document.

### BitLocker Drive Encryption

BitLocker Drive Encryption is a key new security feature in Windows Server 2008 that helps protect servers in remote locations. 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. This prevents someone who runs another operating system, or runs other software tools, from breaking the file and system protections or 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. Checking the integrity of early-boot components helps to ensure that data decryption is performed only if those components appear tamper-free and that the encrypted drive is located in the original computer.

BitLocker offers the option to lock the normal boot process until the user supplies a PIN, much like an ATM card PIN, or he or she inserts a USB flash drive that contains keying material. These added security measures provide multifactor authentication and assurance that the computer will not restart or resume from hibernation until the correct PIN or USB flash drive is presented.

BitLocker also provides enhanced recovery options. BitLocker has a disaster recovery console integrated into the early boot components to provide for data retrieval. In the default setting, BitLocker requires no user actions, and even activation itself can be done remotely and automatically. BitLocker provides a secure and easily manageable data protection solution for the enterprise.

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. The entire system volume is encrypted, including the swap and hibernation files, which provides more security for remote servers in remote locations.

### Enterprise Class Printer Management

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 such as the branch office—from a single interface. This facilitates central management for devices in remote locations where little or no IT staff is available to perform onsite management tasks. More comprehensive coverage of Print Management can be found in Chapter 7, Server Management.

### Windows PowerShell

The 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, even in remote locations such as branch offices. More comprehensive coverage of PowerShell can be found in Chapter 7, Server Management.

### Windows Remote Management

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 remote computers located in branch offices. More comprehensive coverage of Windows Remote Management can be found in Chapter 5, Security and Policy Enforcement

## Improving WAN Efficiency

An ongoing challenge for administrators responsible for managing branch offices is optimizing the available bandwidth and improving the productivity of the workers located in those remote sites. Windows Server 2008 provides several new features and enhancements that will meet this critical need for remote locations.

### TCP/IP Stack

Windows Server 2008 includes a new implementation of the TCP/IP protocol stack known as the Next Generation TCP/IP stack. The Next Generation TCP/IP stack is a complete redesign of TCP/IP functionality for both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) that meets the connectivity and performance needs of today's varied networking environments and technologies. The following features are new or enhanced:

* Receive Window Auto-Tuning and Compound TCP —makes better use of available network bandwidth
* Enhancements for high-loss environments —help make connectivity more consistent and reliable
* Neighbor Unreachability Detection for IPv4 —provides better detection and recovery when network nodes become unavailable
* Changes in Dead Gateway Detection which allow computers to determine of a previously dead gateway has come back online which can result in faster throughput
* Changes to PMTU Black Hole Router Detection —can help prevent connections from termination
* Routing Compartments —allows traffic to be routed in the most efficient way in VPN connection scenarios
* Network Diagnostics Framework support —provides an extensible architecture that helps users recover from and troubleshoot problems with network connections
* Windows Filtering Platform —a new architecture that provides APIs so the Independent Software Vendors (ISVs) can filter at several layers in the TPC/IP protocol stack and throughout the operating system, allowing them to create firewalls, antivirus software, diagnostic software, and other types of applications and services
* Explicit Congestion Notification —can address issues on congested routers, and provide better, more overall throughput

These enhancements help alleviate issues common to remote locations, which are typically connected to Hub sites through lower-speed, and often times less reliable WAN links.

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 through 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. For remote locations, it increases work productivity by providing better transfer times and reducing latency issues normally associated with WAN connections.

#### Receive Window Auto-Tuning

The TCP receive window size is the amount of bytes in a memory buffer on a receiving host that is used to store incoming data on a TCP connection. To correctly determine the value of the maximum receive window size for a connection based on the current conditions of the network, the Next Generation TCP/IP stack supports Receive Window Auto-Tuning. Receive Window Auto-Tuning determines the optimal receive window size per connection by measuring the bandwidth-delay product (the bandwidth multiplied by the latency of the connection) and the application retrieval rate. It then automatically adjusts the maximum receive window size on a regular basis.

With better throughput between TCP peers, utilization of network bandwidth increases during data transfer. If all the applications are optimized to receive TCP data, the overall utilization of the network can increase substantially, making better use of the bandwidth that is available on both Local Area Networks and across WANs that connect remote locations to Hubs.

#### Compound TCP

Whereas Receive Window Auto-Tuning optimizes receiver-side throughput, Compound TCP (CTCP) in the Next Generation TCP/IP stack optimizes sender-side throughput. By working together, they can increase link utilization and produce substantial performance gains for large bandwidth-delay product connections.

CTCP is used for TCP connections with a large receive window size and a large bandwidth-delay product (the bandwidth of a connection multiplied by its delay). It aggressively increases the amount of data sent at a time, yet ensures that its behavior does not negatively impact other TCP connections.

For example, in testing performed internally at Microsoft, backup times for large files were reduced by almost half for a 1 gigabit-per-second connection with a 50-millisecond round-trip time (RTT). Connections with a larger bandwidth-delay product can have even better performance.

#### Enhancements for high-loss environments

The Next Generation TCP/IP stack supports the following Request for Comments (RFCs) to optimize throughput in high-loss environments, such as with Branch Offices connected to Hub sites over WAN links that may experience high latency or be less reliable:

* RFC 2582—The NewReno Modification to TCP's Fast Recovery Algorithm: When multiple segments in a window of data are lost and the sender receives a partial acknowledgement that data was received, the NewReno algorithm provides faster throughput by changing the way that a sender can increase its sending rate.
* RFC 2883—An extension to the Selective Acknowledgement (SACK) Option for TCP: SACK, defined in RFC 2018, allows a receiver to indicate up to four noncontiguous blocks of received data. RFC 2883 defines an additional use of the SACK TCP option to acknowledge duplicate packets. This allows the receiver of the TCP segment containing the SACK option to determine when it has retransmitted a segment unnecessarily and adjust its behavior to prevent future retransmissions. Reducing the number of retransmissions that are sent improves the overall throughput.
* RFC 3517—A Conservative Selective Acknowledgment (SACK)-based Loss Recovery Algorithm for TCP: Whereas Windows Server 2003 and Windows XP use SACK information only to determine which TCP segments have not arrived at the destination, RFC 3517 defines a method of using SACK information to perform loss recovery when duplicate acknowledgements have been received and replaces the fast recovery algorithm when SACK is enabled on a connection. The Next Generation TCP/IP stack keeps track of SACK information on a per-connection basis and monitors incoming acknowledgements and duplicate acknowledgements to more quickly recover when segments are not received at the destination.
* RFC 4138—Forward RTO-Recovery (F-RTO): An Algorithm for Detecting Spurious Retransmission Timeouts with TCP and the Stream Control Transmission Protocol (SCTP): The Forward-Retransmission Timeout (F-RTO) algorithm prevents unnecessary retransmission of TCP segments. Unnecessary retransmissions of TCP segments can occur when there is a sudden or temporary increase in the round-trip time (RTT). The result of the F-RTO algorithm is that for environments that have sudden or temporary increases in the RTT, such as when a wireless client roams from one wireless access point (AP) to another, F-RTO prevents unnecessary retransmission of segments and more quickly returns to its normal sending rate.

Taken together, these improvements facilitate faster, more consistent communications, and result in fewer communications related issues for users and computes in branch offices connecting over WAN links.

#### Changes in dead gateway detection

Dead gateway detection in TCP/IP for Windows Server 2003 and Windows XP provides a failover function, but not a failback function in which a dead gateway is tried again to determine whether it has become available. The Next Generation TCP/IP stack provides failback for dead gateways by periodically attempting to send TCP traffic by using the previously detected dead gateway. If the TCP traffic sent through the dead gateway is successful, the Next Generation TCP/IP stack switches the default gateway to the previously detected dead gateway. Support for failback to primary default gateways can provide faster throughput by sending traffic by using the primary default gateway to a destination. In the branch office scenario, this can result in communications transitioning back to a higher speed primary link between branch and hub sites that had previously been offline, resulting in faster data transfer.

#### Changes in PMTU black hole router detection

Path maximum transmission unit (PMTU) discovery, defined in RFC 1191, relies on the receipt of Internet Control Message Protocol (ICMP) Destination Unreachable-Fragmentation Needed and Don’t Fragment (DF) Set messages from routers containing the MTU of the next link. However, in some cases, intermediate routers silently discard packets that cannot be fragmented. These types of routers are known as black hole PMTU routers. Additionally, intermediate routers might drop ICMP messages because of firewall rules. Due to black hole PMTU routers, TCP connections can time out and terminate.

PTMU black-hole router detection senses when large TCP segments are being retransmitted, and then automatically adjusts the PMTU for the connection, rather than relying on the receipt of the ICMP error messages. In Windows Server 2003 and Windows XP, PMTU black hole router detection is disabled by default because enabling it increases the maximum number of retransmissions that are performed for a specific network segment. The Next Generation TCP/IP stack enables PMTU black hole router detection by default to prevent TCP connections from terminating, which should result in fewer dropped connections for users and computers at branch offices.

### Internet Protocol Version 6 (IPv6)

In Windows Server 2008 and Windows Vista, IPv6 is installed and enabled by default. IPv6 settings can be configured through the properties of the Internet Protocol version 6 (TCP/IPv6) components and through commands in the Netsh interface IPv6 context. IPv6 in Windows Server 2008 and Windows Vista cannot be uninstalled, but it can be disabled.

The Next Generation TCP/IP stack supports a dual IP layer architecture in which the IPv4 and IPv6 implementations share common transport (TCP and UDP) and framing layers. The Next Generation TCP/IP stack has both IPv4 and IPv6 enabled by default. There is no need to install a separate component to obtain IPv6 support.

### Quality of Service

In Windows Server 2003 and Windows XP, Quality of Service (QoS) functionality is made available to applications through the Generic QoS (GQoS) APIs. Applications that used the GQoS APIs accessed prioritized delivery functions. In Windows Server 2008 and Windows Vista, there are new facilities to manage network traffic for both the enterprise and the home.

#### Policy-based QoS for enterprise networks

QoS policies in Windows Server 2008 and Windows Vista allow IT staff to either prioritize or manage the sending rate for outgoing network traffic. IT staff can confine the settings to specific application names, specific source and destination IP addresses, and specific source and destination TCP or UDP ports. QoS policy settings are part of user configuration or computer configuration Group Policy settings and are configured by using the Group Policy Object Editor. They are linked to Active Directory Domain Services containers (domains, sites, and organizational units) by using the Group Policy Management Console.

To manage the use of bandwidth, QoS policy can be configured with a throttle rate for outbound traffic. By using throttling, a QoS policy can limit the aggregate outbound network traffic to a specified rate. To specify prioritized delivery, traffic is marked with a Differentiated Services Code Point (DSCP) value. The routers or wireless access points in the network infrastructure can place DSCP-marked packets in different queues for differentiated delivery. Both DSCP marking and throttling can be used together to manage traffic effectively. Because the throttling and priority marking are taking place at the network layer, applications do not need to be modified.

Using Quality of Service Policies, network administrators can prioritize network traffic from specified users and groups at branch office locations connecting to servers in hub sites. This would take better advantage of available network bandwidth during peak load times, proving faster throughput, a better user experience, and fewer delays, resulting in better overall productivity.

### SYSVOL and Distributed File System Replication (DSFR)

Keeping data updated and synchronized with remote servers is an on-going concern to IT Professionals managing branch office scenarios. Windows Server 2008 includes new replication features to simplify this process.

#### Introduction to DSFR

The Distributed File System Replication (DFSR) service is a multi-master replication engine that is used to keep folders synchronized on multiple servers. Replicating data to multiple servers increases data availability and gives users in remote sites fast, reliable access to files. DFSR uses a compression algorithm called Remote Differential Compression (RDC). RDC is a protocol that can be used to efficiently update files over a limited-bandwidth network. RDC detects insertions, removals, and rearrangements of data in files, enabling DFSR to replicate only the deltas (changes) when files are updated. DFSR is used to replicate Distributed File System and Shared System Volume data. On most types of files, RDC and DFSR can significantly reduce the bandwidth required to maintain data synchronization.

#### SYSVOL and DFSR

In Windows Server 2008, DFSR will replicate the Shared System Volume (SYSVOL) used to store domain information. This introduces several advantages. DFSR is enabled automatically at the Windows Server 2008 domain functionality level. SYSVOL will now get the benefits of remote differential compression, resulting in a reduction in bandwidth utilization.

On-Demand Replication is a new feature in Windows Server 2008 which will replicate only the required files, and it will remove the data from the branch office server if it is not needed. On-Demand Replication can be configured by size or by the last access time. In previous versions of Windows Server, latency between sited connected over lower speed WAN links could cause synchronization issues with things like password resets. This can be avoided by using an On-Demand Replication scheme.

With Windows Server 2008, DFSR and On-Demand Replication combine to provide the needed SYSVOL replication, and conserve bandwidth usage, and reduce unneeded data storage on the branch server.

### Server Message Block 2.0

The Server Message Block (SMB) is the default file-sharing protocol on Windows-based computers and is an extension of the Common Internet File System (CIFS). Windows Server 2008 features SMB version 2.0, which provides Client Side Cache improvements and enhanced file copy performance.

Data transmissions between the client and the server can result in longer wait times for users trying to use applications over the WAN links due to latency. Increased protocol efficiency can’t eliminate latency, but it can minimize its effect and provide branch office workers with a better user experience. SMB 2.0 offers considerable improvement over SMB 1.0, and reduces the impact of latency.

Windows includes an SMB client and an SMB server. SMB version 1.0 was originally designed 15 years ago for early Windows-based network operating systems, such as Microsoft LAN Manager and Windows for Workgroups. SMB in Windows Server 2008 and Windows Vista includes SMB 2.0, a new version of SMB that has been redesigned for today’s networking environments and that meets the needs of the next generation of file servers.

SMB 2.0 supports sending multiple SMB commands within the same packet. This reduces the number of packets sent between an SMB client and server, a common issue with SMB 1.0, reducing the number of times clients and servers must communicate. SMB 2.0 also supports much larger buffer sizes, compared to SMB 1.0., meaning more data can be transferred using fewer packets.

As with all technologies, scalability is an important component. SMB 2.0 bypasses limits of earlier versions, for example, the number of concurrent open file handles on the server is increased, as is the number of file shares that a server can have. Along with scalability, availability is another important component. SMB 2.0 improves availability through support of durable handles that can withstand short interruptions in network availability - allowing users to remain connected, and data transmissions to succeed more often over less reliable links.

The combination of improvements in SMB 2.0 results in faster data transfer times. Some comparative performance statistics taken from Windows Vista (which also natively supports SMB 2.0) are illustrated in the following graphs.

The following figure shows better utilization of network bandwidth, resulting in faster transfer rates on a LAN, downloading and uploading files with SMB 2.0 on compared to SMB 1.0.

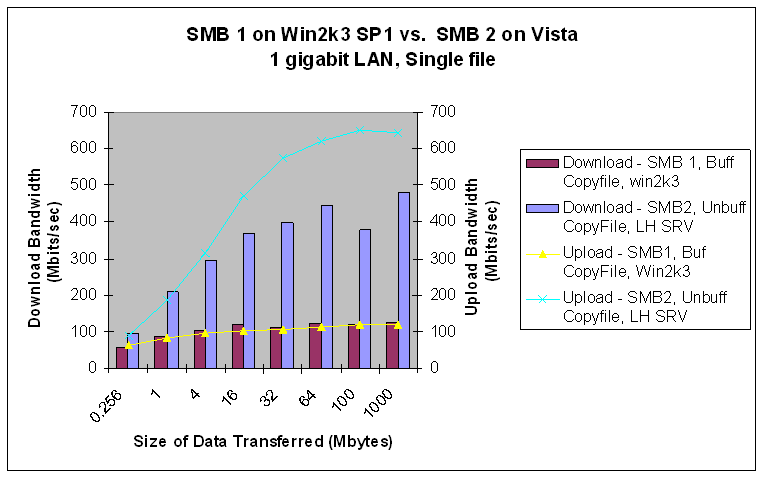


Figure 2: SMB 2.0 compared to SMB 1.0 over a LAN connection

The following figure shows better utilization of network bandwidth, resulting in faster transfer rates over a WAN connection, downloading and uploading files with SMB 2.0 compared to SMB 1.0.

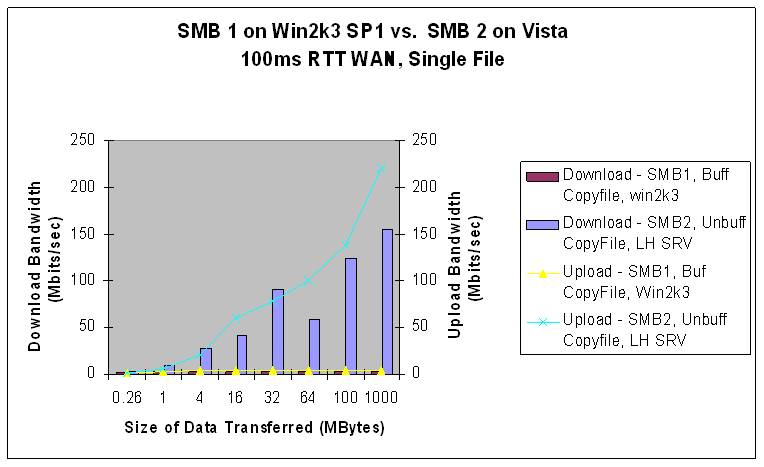


Figure 3: SMB 2.0 compared to SMB 1.0 over a WAN connection

In a remote location scenario, SMB is another key component in Windows Server 2008 that optimizes bandwidth usage and improves connectivity between the remote workers and an organization’s central network.

## Summary

Windows Server 2008, provides new tools and features designed to help IT administrators more effectively deploy and manage servers in branch locations, deal with the growing security needs, and to better utilize the ever-growing bandwidth requirements of the corporate WAN.

New management tools simplify the deployment and administration of Active Directory Domain Services in branch locations, and the Read-Only Domain Controller provides a more secure way to provide domain controller functionality in remote locations. Windows BitLocker Drive Encryption in Windows Server 2008 adds new security options for sensitive data on branch office servers or on remote workers laptops. Organizations can use the new Server Core installation option to provide key server functionality in branch offices with simplified management and improved security.

# Chapter 5: Security and Compliance

## Introduction

Windows Server 2008 offers improved manageability and security compliance through policy-driven security features. Simplified management interfaces allow administrators to easily control the security and policy related functionality, increasing security while reducing management time. Windows Server 2008 has many features that improve security and compliance. Some of the key enhancements include:

* Firewall enhancements—The new Windows Firewall with Advanced Security provides a number of security enhancements.
* Encrypt and protect data—BitLocker protects sensitive data by encrypting the disk drive.
* 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.
* Server and Domain Isolation—Server and domain resources can be isolated to limit access to authenticated and authorized computers.
* Certificate enhancements—Enterprise PKI simplifies certificate management offers improved monitoring abilities, and includes a new Web Enrollment control.
* Enforced client health—Network Access Protection (NAP) enables administrators to configure and enforce health and security requirements before allowing clients access to the network.
* Cryptographic tools—Next Generation Cryptology provides a flexible cryptographic development platform.
* Manage user identities—Identity and access solutions are a set of platform technologies designed to help organizations manage user identities and access privileges
* Federated Rights Management—Federated collaboration simplifies the secure sharing of sensitive information with external users.
* 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.

## Windows Firewall Advanced Security

The Windows Firewall with Advanced Security in Windows Server 2008 reduces conflicts and coordination overhead between technologies. Windows Firewall with Advanced Security provides centralized firewall filtering and connection security rules. It 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 a level of protection from malicious users and programs on a network. The advanced security functionality of Windows Firewall includes:

* Support for both incoming and outgoing traffic
* A new Microsoft Management Console (MMC) snap-in for local and remote firewall configuration
* Integrated firewall filtering and Internet Protocol security (IPSec) protection settings
* Many new ways to configure firewall exceptions

#### Support for both incoming and outgoing traffic

Currently, Windows Firewall supports the use of the firewall for intercepting incoming traffic, dropping all unsolicited incoming traffic that does not correspond either to traffic sent in response to a request (solicited traffic) or unsolicited traffic that has been specified as allowed (excepted traffic). This is a crucial component of firewall functionality as it helps prevent the infection of computers by network-level viruses and worms that spread through unsolicited incoming traffic.

A feature of the advanced security functionality in Windows Firewall in Windows Server 2008 is ability to support firewall interception of both incoming and outgoing traffic. For example, a network administrator can configure the new Windows Firewall with a set of exceptions to block all traffic sent to specific ports, such as the well-known ports used by virus software, or to specific addresses containing either sensitive or undesirable content. The default behavior of Windows Firewall in Windows Server 2008 is to:

* Block all incoming traffic unless it is solicited or it matches a configured exception
* Allow all outgoing traffic unless it matches a configured exception

#### This further helps protect the network as well as other systems from a computers that becomes infected with a virus.

#### New MMC snap-in for GUI configuration

Windows Firewall is now configured with an MMC snap-in named Windows Firewall with Advanced Security. With this snap-in, network administrators can configure settings for Windows Firewall on local and remote computers (which is not possible for the current Windows Firewall without a remote desktop connection). Moreover, administrators can use commands in the netsh advfirewall context for command-line configuration of advanced settings of the new Windows Firewall.

#### Integrated firewall and IPSec settings

IPSec is a set of Internet standards to provide cryptographic protection for IP traffic. 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 has combined the configuration of both network services using the same GUI and command-line commands. This integration of firewall and IPSec settings also simplifies the configuration of IPSec settings.

#### Several ways to configure firewall exceptions

The advanced security functionality in Windows Server 2008 allows administrators to configure firewall exceptions in many new ways:

* Exceptions can be configured for IP protocol number. The new Windows Firewall allows administrators to either select the protocol by name or manually type the value of the IPv4 Protocolor IPv6 Next Headerfields for the desired traffic.
* Exceptions can be configured for source and destination. Administrators can configure both source and destination TCP or UDP ports for both incoming and outgoing traffic, allowing them to more closely define the type of TCP and UDP traffic that is allowed or blocked.
* Exceptions can be configured for all or multiple ports. Administrators can also specify all TCP or UDP ports (for all TCP or all UDP traffic) or a comma-delimited list of multiple ports.
* Exceptions can be configured for specific types of interfaces.Administrators can specify that an exception applies to all interfaces or to specific types of interfaces, including LAN, remote access, or wireless interfaces.
* Exceptions can be configured for ICMP and ICMPv6 (ping) traffic by Type and Code. With Windows Firewall in Windows Server 2008, there is a predefined set of commonly excepted ICMP and ICMPv6 messages, and administrators can add new ICMP or ICMPv6 messages by specifying the ICMP or ICMPv6 message Type and Code field values. For example, if an administrator wanted to create an exception for the ICMPv6 Packet Too Big message, she or he could manually create an exception for ICMPv6 Type 2 and Code 0.
* Exceptions can be configured for services. Administrators can specify that the exception applies to any process, to services only, to a specific service by its service name, or administrators can type the short name for the service. For example, if an administrator wanted to configure an exception to apply only to the Computer Browser service, he or she could select the Computer Browser service from the list of services running on the computer.

The new Windows Firewall included in Windows Server 2008 intercepts outgoing traffic to well-known ports used by virus software, or to specific address containing either sensitive or undesirable content, helping to prevent the spread of viruses within an organization and protecting key systems. The new Windows Firewall with Advanced Security MMC snap-in allows administrators to more easily configure both Windows Firewall and IPSec settings on local and remote systems. There are also several new ways to configure Windows Firewall exceptions introduced, providing administrator’s flexibility to respond to new security threats. These improvements provide enhanced security and easier administration of Windows Firewall in Windows Server 2008.

## BitLocker Drive Encryption

BitLocker Drive Encryption is a key new security feature in Windows Server 2008 that helps 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 someone who runs a parallel operating system, or runs other malicious software tools, from breaking the file and system protections, or from performing offline viewing of the files stored on the protected drive. More comprehensive coverage of BitLocker can be found in Chapter 4, Branch Office.

## Active Directory Domain Services: Auditing

In Windows Server 2008, Administrators have more options for auditing access to Active Directory objects. The new audit policy subcategory (Directory Service Changes) audits changes to Active Directory objects, such as creation, modification, movement, and undeletion, and logs the old and new attribute values when changes are made.

Note: Audit directory service access is applied in the same manner as Audit object access; however, it applies only to AD DS objects and not to file system objects and registry objects.

### Auditing AD DS access

In Windows 2000 Server and Windows Server 2003, there was one audit policy, Audit directory service access. It controlled whether auditing for directory service events was enabled or disabled. In Windows Server 2008, this policy is divided into four subcategories:

* Directory Service Access
* Directory Service Changes
* Directory Service Replication
* Detailed Directory Service Replication

The global audit policy Audit directory service access controls whether auditing for directory service events is enabled or disabled. This security setting determines whether events are logged in the Security log when certain operations are carried out on objects in the directory. Administrators can control what operations to audit by modifying the system access control list (SACL) on an object. The SACL on an AD DS object can be set on the **Security** tab of that object's properties dialog box. In Windows Server 2008, this policy is enabled by default.

If this policy setting is defined (by modifying the default Domain Controllers Policy), the administrator can specify whether to audit successes, audit failures, or not audit at all. Success audits generate an audit entry when a user successfully accesses an AD DS object that has a SACL specified. Failure audits generate an audit entry when a user unsuccessfully attempts to access an AD DS object that has a SACL specified. In Windows 2000 Server and Windows Server 2003 audit events appeared in the Security log with the ID number 566. In Windows Server 2008, the audit policy subcategory Directory Service Access still generates the same events, but the event ID number is changed to 4662.

### Auditing AD DS Changes

The new audit subcategory Directory Service Changes enables the ability to audit changes to objects in AD DS. The types of changes that can be audited are create, modify, move, and restore operations that are performed on an object. The events that are generated by these operations appear in the Security log, and include the previous and current attribute values.

This new policy subcategory adds the following capabilities to auditing in AD DS:

* When a successful modify operation is performed on an attribute of an object, AD DS logs the previous and current values of the attribute. If the attribute has more than one value, only the values that change as a result of the modify operation are logged.
* If a new object is created, values of the attributes that are populated at the time of creation are logged. If attributes are added during the create operation, those new attribute values are logged. In most cases, AD DS assigns default values to attributes (such as sAMAccountName). The values of such system attributes are not logged.
* If an object is moved within a domain, the previous and new location (in the form of the distinguished name) is logged. When an object is moved to a different domain, a create event is generated on the domain controller in the target domain.
* If an object is restored, the location to which the object is moved is logged. In addition, if attributes are added, modified, or deleted during a restore operation the values of those attributes are logged.

If an object is deleted, no change auditing events are generated. However, an audit event is generated if the Directory Service Access subcategory is enabled.

After Directory Service Changes is enabled, AD DS logs events in the Security event log when changes are made to objects that an administrator has set up for auditing. The following table describes these events.

Table 8: AD DS log events

|  |  |  |
| --- | --- | --- |
| Event ID | Type of event | Event description |
| 5136 | Modify | This event is logged when a successful modification is made to an attribute in the directory. |
| 5137 | Create | This event is logged when a new object is created in the directory. |
| 5138 | Restore | This event is logged when an object is restored in the directory. |
| 5139 | Move | This event is logged when an object is moved within the domain. |

### Global audit policy

Audit policy helps track and audit all events and application usages in the server. It also allows administrators to configure, create, back-up and restore audit policies on any computer within the organization.

Enabling the global audit policy Audit directory service access enables all the directory service policy subcategories. This global audit policy can be set in the Default Domain Controllers Group Policy (under Security Settings\Local Policies\Audit Policy). In Windows Server 2008, this global audit policy is enabled by default. Therefore, the subcategory Directory Service Changesis also enabled by default. This subcategory is set only to audit success events. The two audit subcategories are, however, independent of each other. Administrators can choose disable Directory Service Access and still be able to see change events that are generated if the subcategory Directory Service Changes is enabled.

In Windows 2000 Server and Windows Server 2003, the policy Audit directory service access was the only auditing control available for Active Directory. The events that were generated by this control did not show the old and new values of any modifications. With the new audit policy subcategory Directory Service Changes, successful changes to the directory are logged along with the previous and current attribute values. The ability to identify how object attributes change makes the event logs more useful as a tracking mechanism for changes that occur over the lifetime of an object and to revert back to previous attribute values if necessary.

## 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.

## Read-Only Domain Controllers (RODCs)

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 authenticated and authorized computers. 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 in order 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.

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 domain member computers accept only authenticated and secured communications from other domain member computers. 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.

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.

## Enterprise PKI

There are a number of enhancements to the public key infrastructure (PKI) in the Windows Server 2008 and Windows Vista operating systems. There have been improvements in manageability throughout all aspects of Windows PKI, certificate revocations services have been redesigned, and there is a decreased attack surface for enrolment. PKI enhancements include:

* Easier Management through PKIView
* Certificate Web Enrollment
* Network Device Enrollment Service
* Certificate Policy Settings
* Certificate Deployment changes
* Online Certificate Status Protocol (OCSP) support
* Managing Certificates with Group Policy

These enhancements in Windows Server 2008 offer new options and functionality for IT Professionals managing an organization’s PKI environment.

### Enterprise CA Management with PKIView

Originally part of the Microsoft Windows Server 2003 Resource Kit and called the PKI Health tool, PKIView is 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 CA certificates published in AD CS. Because it is part of the core operating system of Windows Server 2008, administrators can use PKIView after server installation by simply adding it to MMC. PKIView is then available to analyze the health state of CAs and to view details for CA certificates published in AD CS.

PKIView provides a view of the status of the network's PKI environment. Having a view of all CAs and their current health states enables administrators to manage CA hierarchies and troubleshoot CA errors more easily and effectively. Specifically, PKIView indicates the validity or accessibility of authority information access (AIA) locations and certificate revocation list (CRL) distribution points (CDP).

For each CA selected, PKIView indicates CA health states in the tree as follows:

Table 9: PKIView CA health states

| **Indicator** | **CA State** |
| --- | --- |
| Question Mark | CA health state evaluation |
| Green indicator | CA has no problems |
| Yellow indicator | CA has a non-critical problem |
| Red indicator | CA has a critical problem |
| Red Cross over CA icon | CA is offline |

After the PKIView snap-in is added to the MMC, administrators can see three panes:

* Tree—This pane displays a tree representation of the network’s PKI hierarchy. Each node under the Enterprise PKI node represents a CA with subordinate CAs as child nodes.
* Results—For the CA selected in the tree, this pane displays a list of subordinate CAs, CA certificates, CRL distribution points (CDPs), and AIA locations. If the console root is selected in the tree, the results pane displays all root CAs. There are three columns in the Results pane:
  + Name—If the Enterprise PKI node is selected, the names of the root CAs under the Enterprise PKI node are displayed. If a CA or child CA is selected in the tree, then the names of CA certificates, AIA locations, and CDPs are displayed.
  + Status—Provides a brief description of CA status (also indicated in the tree by the icon associated with the selected CA) or the status of CA Certificates, AIA locations, or CDPs (indicated by status text descriptions, examples of which are OK and Unable to Download).
  + Location—Shows AIA locations and CDPs (protocol and path) for each certificate. Examples are file://, HTTP://, and LDAP://.
* Actions—This pane provides the same functionality found on the Actions**,** View**,** and Help menus.

Depending on the item selected in either the tree or Results pane, users can view more details about CAs and CA certificates including AIA and CRL information in the Actions pane. They can also manage the enterprise PKI structure and make corrections or changes to CA certificates or CRLs.

### Certificate Services

Certificate Services provides customizable services for issuing and managing certificates used in software security systems employing public key technologies. Windows Vista and Windows Server 2008 introduce new functionality for Certificate Services, including a new COM enrollment control, a new enrollment DLL, and the introduction of Simple Certificate Enrollment Protocol (SCEP), a public key infrastructure (PKI) communication protocol.

### Certificate Web Enrollment

Many changes have been made to certificate Web enrollment support in Windows Server 2008. The previous ActiveX enrollment control was replaced with a new COM enrollment control for Windows Vista and Windows Server 2008.

Certificate Web enrollment has been available since Windows 2000 operating systems. It is designed to provide an enrollment mechanism for organizations that need to issue and renew certificates for users and computers that are not joined to the domain or are not connected directly to the network, and for users of non-Microsoft operating systems. Instead of relying on the auto-enrollment mechanism of a certification authority (CA) or using the Certificate Request Wizard, the Web enrollment support provided by a Windows-based CA allows these users to request and obtain new and renewed certificates over an Internet or intranet connection.

#### Changed functionality

The previous enrollment control, XEnroll.dll, has been removed from Windows Vista and Windows Server 2008, and a new enrollment control, CertEnroll.dll, was introduced in its place. Although the Web enrollment process is essentially the same, this change in enrollment controls can have an impact on compatibility when users or computers running Windows Vista or Windows Server 2008 attempt to request a certificate by using Web enrollment pages installed on those earlier versions of Windows.

Windows Server 2008 CAs will continue to support certificate Web enrollment requests from users on Windows XP and Windows Server 2003 clients. If users are enrolling certificates through the Windows Server 2008 Web enrollment pages from a Windows XP, Windows Server 2003, or Windows 2000-based computer, the Web enrollment pages will detect this and use the Xenroll.dll that was installed locally on the client. However, the following client behaviors will be different than in earlier versions of Windows:

* Enrollment agent capability (also referred to as the smart card enrollment station) was removed from Web enrollment in Windows Server 2008 because Windows Vista provides its own enrollment agent capability. If users need to perform enrollment on behalf of another client with a Windows Server 2008 Web enrollment, they should use computers running Windows Vista as enrollment stations. Alternatively, they can use a Windows Server 2003-based server with Web enrollment installed and use that server as an enrollment agent to enroll certificates through a Windows Server 2008 CA.
* Only users of Internet Explorer version 6.x or later, or Netscape 8.1 browser can submit certificate requests directly through the Web enrollment pages. Users of other Web browsers can still submit enrollment requests by using the Web enrollment pages, but they must first pre-generate a PKCS#10 request for submission through the Web enrollment pages.
* Certificate Web enrollment cannot be used with version 3.0 certificate templates, which are introduced in Windows Server 2008 to support the issuance of suite b-compliant certificates.
* Internet Explorer cannot run in the local computer's security context; therefore, users can no longer request computer certificates by using Web enrollment.

### Network Device Enrollment

The Network Device Enrollment Service (NDES) is Microsoft's implementation of the Simple Certificate Enrollment Protocol (SCEP), and used to be called Microsoft Simple Certificate Protocol (MSCEP). SCEP is a public key infrastructure (PKI) communication protocol that makes it possible for software running on network devices such as routers and switches, which cannot otherwise be authenticated on the network, to enroll for x509 certificates from a certification authority (CA). Microsoft SCEP (MSCEP) is the Windows implementation of SCEP.

MSCEP operates as an Internet Server Application Programming Interface (ISAPI) filter on Internet Information Services (IIS) that performs the following functions:

* Generates and provides one-time enrollment passwords to administrators
* Receives and processes SCEP enrollment requests on behalf of software running on network devices
* Retrieves pending requests from the CA

In Windows Server 2003, MSCEP was a Windows Server 2003 Resource Kit add-on that had to be installed on the same computer as the CA. In Windows Server 2008, MSCEP is part of the operating system and can be installed on a different computer than the CA.

With NDES and SCEP, organizations can enhance the security by allowing network devices such as routers and switches to be authenticated.

### Managing Certificates with Group Policy

Software signing is being used by a growing number of software publishers and application developers to verify that their applications come from a trusted source. However, many users do not understand or pay little attention to the certificates associated with applications that they install. As X.509 public key infrastructures become more widely used as a foundation of trust, many organizations need more options to manage certificate path discovery and path validation. Certificate settings in Windows Server 2008 Group Policy enable administrators to manage certificate validation settings according to the security needs of the organization and manage the certificate settings on all the computers in the domain from a central location.

For example, in situations where certain intermediate certification authority (CA) certificates expire and clients cannot automatically retrieve a new certificate, administrators can now deploy these certificates to client computers through Group Policy. Another relevant scenario is when administrators want to ensure that users never install applications that have been signed with unapproved publisher certificates.

This feature applies to organizations that have public key infrastructures (PKIs) with one or more Windows-based CAs and use Group Policy to manage client computers.

Using certificate validation settings in Group Policy allows:

* Security architects to enhance the use of certificate-based trusts
* Security administrators to manage PKI-enabled applications in their environment

Using certificate trust–related Group Policy settings requires careful planning to determine the certificate needs of users and computers in the organization, and the amount of control they should have over those certificates. Administrators might be able to provide users with greater leeway if they combine the use of these settings with clear and effective training so that users understand the importance of certificates, the risks of poor certificate management, and how to manage their certificates responsibly.

### Certificate-related Group Policy Settings

Previous versions of Windows operating systems had few settings to implement this kind of control over certificate validation. Certificate-related Group Policy settings can be found in the Group Policy Object Editor, under Computer Configuration\Windows Settings\Security Settings\Public Key Policies**.** The following policy options can be managed under separate tabs on the Certificate Path Validation Settings properties sheet:

* Stores
* Trusted Publishers
* Network Retrieval
* Revocation

In addition, four new policy stores have been added under Public Key Policies for use in distributing different types of certificates to clients:

* Intermediate Certification Authorities
* Trusted Publishers
* Untrusted Certificates
* Trusted People

These new policy stores are in addition to the Enterprise Trust and Trusted Root Certification Authorities stores that were available in Windows Server 2003. These path validation settings and certificate stores can be used to complete the following tasks:

* Managing the peer trust and trusted root certificate stores
* Managing trusted publishers
* Blocking certificates that are not trusted according to policy
* Managing retrieval of certificate-related data
* Managing expiration times for CRLs and online certificate status protocol (OCSP) responses
* Deploying certificates

### Managing peer trust and trusted root CA stores

By using the Stores tab on the Certificate Path Validation Settings dialog box, administrators can regulate the ability of users to manage their own trusted root certificates and peer-trust certificates. This control can be implemented so that users are not allowed to make any root or peer-trust decisions, or it can be used to control how many or how few specific certificate purposes, such as signing and encryption, users can manage for peer trust.

The Stores tab also allows administrators to specify whether users on a domain-joined computer can trust only enterprise root CAs, or both enterprise root and non-Microsoft root CAs. If, on the other hand, an administrator needs to distribute selected trusted root certificates to computers in the domain, they can do so by copying them into the trusted root certificate store. They will then be propagated to the appropriate certificate store the next time domain policy is refreshed.

Because of the growing variety of certificates in use today and the growing importance of decisions that need to be made about whether to recognize or not recognize these certificates, some organizations might want to manage certificate trust and prevent users in the domain from configuring their own set of trusted root certificates.

### Managing trusted publishers and blocking unwanted certificates

The policy options in the Trusted Publisherstab of theCertificate Path Validation Settings dialog box allow administrators to control which certificates can be accepted as coming from a trusted publisher. Specifying organization-wide trusted publisher policy options allows organizations to decide whether Authenticode certificates can be managed by users and administrators, only administrators, or only enterprise administrators.

Administrators can prevent certain certificates from ever being used in their organization by adding them to the Untrusted Certificates store. Just as network administrators are responsible for preventing viruses and other malicious software from entering their environments, administrators in the future might want to block certain certificates from being used. A certificate issued by the organization’s own CA can be revoked, and it will be added to a certificate revocation list. Certificates issued by external CAs cannot be revoked. However, these untrusted certificates can be disallowed by adding them to the Untrusted Certificates store. These certificates will be copied to the Untrusted Certificates store of each client computer in the domain the next time Group Policy is refreshed.

### Certificate Deployment Changes

User and computer certificates can be deployed by using a number of mechanisms, including auto-enrollment, the Certificate Request Wizard, and Web enrollment. Deploying other types of certificates to a large number of computers, however, can be challenging. In Windows Server 2003 it was possible to distribute trusted root CA certificate and enterprise trust certificates by using Group Policy.

In Windows Server 2008, all of the following types of certificates can be distributed by placing them in the appropriate certificate store in Group Policy:

* Trusted root CA certificates
* Enterprise trust certificates
* Intermediate CA certificates
* Trusted publisher certificates
* Untrusted certificates
* Trusted people (peer-trust certificates)

This provides administrators with an efficient means of distributing the growing variety of certificates to users and computers in their organizations.

### Online Certificate Status Protocol Support

Certificate revocation is a necessary part of the process of managing certificates issued by certification authorities. The most common means of communicating certificate status is by distributing certificate revocation lists (CRLs). In situations where the use of conventional CRLs is not an optimal solution, Online Certificate Status Protocol (OCSP) support in Windows Server 2008 can be used to manage and distribute revocation status information.

#### What OCSP Support Does

Online Certificate Status Protocol responses and the use of CRLs are two common methods for conveying information about the validity of certificates. Unlike CRLs, which are distributed periodically and contain information about all certificates that have been revoked or suspended, an online responder only receives and responds to requests from clients for information about the status of a single certificate. The amount of data retrieved per request remains constant no matter how many revoked certificates there might be.

In many circumstances, online responders can process certificate status requests more efficiently than by using certificate revocation lists. Examples of the kind of circumstances include:

* Clients connect to the network remotely and either do not need, nor have the high-speed connections required, to download large CRLs.
* A network needs to handle large peaks in revocation checking activity, such as when large numbers of users log on or send signed e-mail messages simultaneously.
* An organization needs an efficient means to distribute revocation data for certificates issued from a non-Microsoft CA.
* An organization wants to provide only the revocation checking data needed to verify individual certificate status requests, rather than make available information about all revoked or suspended certificates.

OCSP support in Windows Server 2008 includes the following.

* Web proxy caching—The online responder Web proxy cache is the service interface for the online responder. It is implemented as an Internet Server API (ISAPI) Extension hosted by Internet Information Services (IIS).
* Support for nonce and no-nonce requests—Configuration options for nonce and no-nonce request can be used to prevent replay attacks of OCSP responses.
* Windows setup integration—Online responders can be set up by using the Windows Server Role Management Tool.
* Advanced cryptography support—An OCSP responder can be configured to use elliptic curve cryptography (ECC) and SHA-256 cryptography for cryptographic operations.
* Preconfigured OCSP certificate templates—Deploying an OCSP responder is simplified by using an OCSP certificate template available in Windows Server 2008.
* Kerberos protocol integration—OCSP requests and responses can be processed along with Kerberos password authentication for prompt validation of server certificates at logon.

Microsoft online responders are based on and comply with RFC 2560 for OCSP. For this reason, certificate status responses from online responders are frequently referred to as OCSP responses.

### Functionality Provided by OCSP

Two significant new sets of functionality can be derived from online responder services:

* Online responders—The basic online response functionality provided by a single computer where OCSP services have been installed.
* Responder arrays—Multiple linked computers hosting online responders and processing certificate status requests.

An online responder is a computer on which the OCSP service is running. A computer that hosts a CA can also be configured as an online responder, but it is recommended that users maintain CAs and online responders on separate computers. A single online responder can provide revocation status information for certificates issued by a single CA or multiple CAs. CA revocation information can be supported by more than one online responder.

Applications that depend on X.509 certificates, such as Secure/Multipurpose Internet Mail Extensions (S/MIME), Secure Sockets Layer (SSL), Encrypting File System (EFS), and smart cards need to validate the status of the certificates whenever they are used to perform authentication, signing, or encryption operations. Certificate status and revocation checking verifies the validity of certificates based on:

* Time—Certificates are issued to a fixed period of time and considered valid as long as the expiration date of the certificate is not reached and the certificate has not been revoked before that date.
* Revocation status—Certificates can be revoked before their expiration date for a variety of reasons, such as key compromise or suspension.

Certificate revocation lists contain the serial numbers of all of the certificates issued by a CA that have been revoked. For a client to check the revocation status of a certificate, it needs to download a CRL containing information about all of the certificates that have been revoked by the CA.

### Group Policy Settings for OSCP

Several Group Policy settings have been added to enhance management of OCSP and CRL data use. CRLs have expiration dates just like certificates. If the expiration date passes before an update is published or becomes accessible, certificate chain validation can fail, even with an Online Responder present. This is because the Online Responder would be relying on data from an expired CRL. In situations where network conditions can delay the timely publication and receipt of updated CRLs, administrators can use these Group Policy settings to extend the expiration time of an existing CRL or OCSP response.

The lifetime of CRLs and OCSP responses can be extended by going to the Revocationtab inCertificate Path Validation Settings(Computer Configuration**,** Windows Settings**,** Security Settings**,** andPublic Key Policies) and configuring two options:

* Allow for all CRLs and OCSP responses to be valid longer than their lifetime
* Default time the validity period can be extended

A separate option on the **Revocation** tab allows the OCSP responses to be overridden with information contained in CRLs. This allows a certificate that has been revoked by adding it to a local CRL to still be verified as valid if a client has a CRL that does not include its revocation status. Although this option is not recommended, it can be useful in circumstances where revocation changes made by a local administrator are not final until a CA administrator verifies the change.

### 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. Historically, static V1 certificate templates were introduced with Windows 2000 Server. With Windows Server 2003, customization was introduced with V2 certificate templates. 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 are also running on Windows Server 2008. Additionally, only Windows Vista client computers and Windows Server 2008 computers can enroll for V3 certificate templates.

Table 10

|  |  |  |
| --- | --- | --- |
| **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 2000 Enterprise Edition  Windows Server 2003 Enterprise Editiion  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.

### 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 (AD CS), 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, which is supported by Windows Server 2008 and Windows Vista, has the following capabilities:

* CNG allows customers to use their own cryptographic algorithms or implementations of standard cryptographic algorithms. Customers can also add new algorithms.
* CNG supports cryptography in kernel mode. The same API is used in both kernel mode and user mode to fully support cryptography features. Secure Sockets Layer/Transport Layer Security (SSL/TLS) and IPSec, in addition to startup processes that use CNG, operate in kernel mode.
* The plan for CNG includes acquiring Federal Information Processing Standards (FIPS) 140-2 level-2 certification, together with Common Criteria evaluations.
* CNG complies with Common Criteria requirements by using and storing long-lived keys in a secure process.
* CNG supports the current set of CryptoAPI 1.0 algorithms.
* CNG provides support for elliptic curve cryptography (ECC) algorithms. A number of ECC algorithms are required by the United States government's Suite B effort.
* Any computer with a Trusted Platform Module (TPM) will be able to provide key isolation and key storage in TPM.

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 the Suite B see: http://www.nsa.gov/ia/industry/crypto\_suite\_b.cfm

## Identity and Access Management 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 cannot 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 poorly constructed 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

Microsoft 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 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 key 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
  + Federated Rights Management
* Strong Authentication
  + Cryptography API
  + V3 certificate templates
  + Public Key Infrastructure (PKI)

### Active Directory Rights Management Services

Windows Server 2008 Active Directory Rights Management Services (AD RMS) (formerly Windows RMS) is a key to providing protection for sensitive information. Prior to the release of Windows Server 2008, sharing an RMS-protected document with a user outside the corporate network required the recipient to have a compatible RMS server inside their own organization. Alternatively, the outside user could be given an Active Directory account *inside* the corporate network, a process that presents challenging administrative and security issues. The Microsoft collaboration platform, Microsoft Office SharePoint Server 2007, was also capable of dynamically applying RMS protection to documents based on the Active Directory profiles of users, but this required a local Active Directory account as well.

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 to 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. Once external users are authenticated, RMS will automatically provide all appropriate licenses to allow external users to work with and organization’s sensitive internal content. Administrators gain granular control over how these external users interact with protected content, including the ability to define templates that can apply to multiple partners’ relationships.

In Windows Server 2008, AD FS and AD RMS work together to enable users from different domains to securely share documents based on federated identities, rather than local Active Directory profiles. It can interpret AD FS claims to authenticate users and control their access to content. When external users sign in to their local Active Directory domains, they are provided with federation claims that contain their credentials and the access rights that they should be granted.

This creates a powerful new content sharing scenario—federated document collaboration—that eliminates the need to maintain shadow accounts for external users and provides those users with single sign-on access to RMS-protected content. After two entities have set up a federated trust, users can share and utilize protected content almost as if they were in the same domain. Administrators at the resource provider can control the fine points of who has what kind of access to what kinds of content without needing to manage identities for individual users.

### 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. The user is required to enter secondary credentials when he or she attempts 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 (B2B) 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 only.

AD FS includes a policy import/export feature to make it easier to set up a trust relationship between federation partners. A membership provider allows role based authorization to Windows SharePoint Services and RMS for users from a federation partner. Administrators have the ability to control federation service deployment through group policy. Support for different certificate-revocation checking settings is now provided as well.

In addition, organizations that own and manage user accounts can deploy AD FS federation servers that authenticate local users and create security tokens. Federation servers in the resource organization can use these security tokens to make authorization decisions.

### Persistent Information Protection

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 Web sites, and e-mail messages. 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.

The AD RMS server and client system handles the process, beginning with issuing users permission to apply RMS permissions to content in the first place. When an individual has been issued a rights account certificate by the RMS server, that user can protect content. Enabling RMS protection of a document is simple; RMS features are built into Microsoft productivity applications like Microsoft Office Word and Microsoft Office Excel. The RMS server binds the rights information to the content and encrypts the content to prevent unauthorized access. When a user attempts to view or otherwise use protected documents, the RMS server is alerted and checks the user’s permissions, issuing decryption and use licenses as appropriate.

Prior to Windows Server 2008, an external user needing to access RMS-protected content had to have a local user account. This is no longer necessary, which simplifies management of external accounts.

### Scenario: Secure and Easy Collaboration

With the Microsoft Federated Rights Management solution, secure collaboration of shared content is easier to manage and the protection of the organization’s critical data is increased. A common collaboration scenario involves companies that need to share confidential information with employees of another organization. Contoso, for example, may be designing a new product and wishes to have engineers at Fabrikam review product specifications and prepare a plan for production. The specifications are confidential, and Contoso wants the engineers to be able to read them, but not alter, copy, print, or forward them.

Using the integrated RMS features in Office Word 2007, the product manager at Contoso can easily apply the appropriate permissions. If the two companies are using AD FS in Windows Server 2008 and share a federated trust. Contoso applies the RMS permissions as before, but there is no need to provide the Fabrikam employees with local Active Directory identities. When the employees sign in to Fabrikam’s domain, they are provided with AD FS claims which can be interpreted by Contoso’s AD RMS server once they are authorized as a federated user.

### Federated Rights Management Summary

In a collaborative world, sharing information without breaking security policy is an evolving challenge. The inclusion of RMS technology in Windows Server 2008 was a significant step towards achieving secure collaboration, as was the development of AD FS. Now, the integration between the AD RMS and AD FS allows companies to share information securely more easily than ever before. By enabling RMS and Office SharePoint Server 2007 to interpret AD FS claims, administrators no longer face the security and management headaches of maintaining redundant Active Directory stores.

AD RMs helps prevent unauthorized use of documents, data and emails. RMS enables document owners to identify authorized users and manage restrictions on the usage of documents.

## Other security enhancements

There are many other enhancements in Windows Server 2008 that can help organizations improve the security of their servers and network.

### Code integrity

Code integrity helps protect the operating system files when the operating system is running by signing all operating system executables and DLLs. These signatures are then checked for validity when files are loaded into memory.

### Windows Service Hardening

Windows Server 2008 hardens the operating system and protects the environment to provide a solid foundation for running and business applications and services. Windows Service Hardening helps keep systems safer by preventing critical Windows services from being used by abnormal activity in the file system, registry, or network. With Windows Service Hardening fewer services are running by default, and service accounts now have fewer privileges and limited network access.

In Windows Server 2008 also provides better protection for kernel mode services by reducing amount of code that has to run at the kernel level. For example, in the past there have been some printer drivers that used both kernel-mode code and user-mode code. With service hardening, printer drivers have been moved into the user-mode layer which means that there is no kernel code in the drivers themselves. By ensuring that services run with the least privilege necessary, service hardening improves the system security.

Windows Service Hardening prevents critical Windows services from being used by abnormal activity in the file system, registry, or network. Service hardening reduces the risk of the platform being intruded.

### Windows Server Core

Server Core is a minimal installation of Windows Server with specific functionality and without any unneeded features. Server Core is covered in the Server Management section of this paper.

### Removable device installation

Windows Server 2008 provides companies with a way to protect data from being copied onto a removable device such as a USB drive. Group Policy settings can be configured to determine control of keyboard, mice, or USB drives. Administrators can have flexibility in determining how removable devices may or may not be used, including:

* Preventing users from installing any device
* Allowing users to install only devices that are on an “approved list. If a device is not on the list, then the user cannot install it.
* Preventing users from installing devices that are on a “prohibited” list. If a device is not on the list, then the user can install it.
* Denying read or write access to users for devices that are themselves removable, or that use removable media, such as CD and DVD burners, floppy disk drives, external hard drives, and portable devices such as media players, smart phones, or Pocket PC devices

Restricting the devices that users can install can help reduce the risk of data theft, and it can lower support costs by ensuring that users are installing only devices that the help desk is trained and equipped to support.

## Network Access Protection (NAP)

Simply put, 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 those clients can connect to the corporate network. NAP also provides a suite of APIs that allow companies other than Microsoft to integrate their software into the NAP platform. By using the NAP APIs, software developers and vendors can customize the capabilities of NAP with additional compliance validation and enforcement mechanisms.

### An Introduction to Network Access Protection?

Most organizations create network policies that specify the type of hardware and software that can be deployed on the network. These policies frequently include rules for how client computers can and cannot be configured before connecting to the network. For example, many organizations require that client computers must run antivirus software with recent antivirus updates installed, and that client computers must have a software firewall installed and enabled before connecting to the organization’s network. A client computer that is configured according to the organization network policy is viewed as being compliant with health policy, while a computer that is not configured according to the organization’s network policy is viewed as being noncompliant with health policy.

NAP allows administrators to use Network Policy Server (NPS) to create policies that define client computer health. NAP also enforces client health policies defined by the organization. This protects the network from harmful elements introduced by client computers, such as computer viruses. NAP can also automatically update NAP-capable client computers through automatic remediation to bring the clients into compliance with client health policy. NAP also provides continuous detection of client computer health to guard against circumstances in which a client computer is compliant when it connects to the organization network but becomes noncompliant while connected.

NAP deployments require servers that are running Windows Server 2008. In addition, client computers must be running Windows Vista, Windows Server 2008, Windows Server 2003 SP1 or Windows® XP with Service Pack 2 (SP2) with Network Access Protection Client for Windows XP installed.

### NAP architecture

The NAP architecture consists of both client and server components, and is shown in the following illustration:

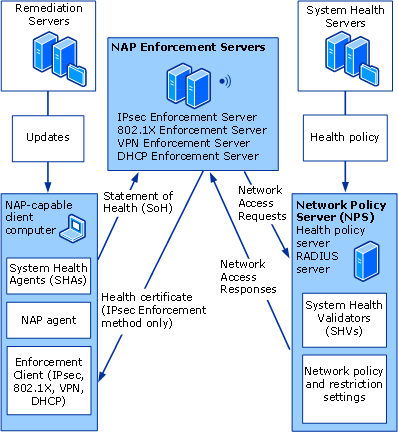


Figure 4: NAP architecture client and server components

### NAP components

NAP consists of multiple client and server components. There are common NAP components that are used in all NAP deployments, and there are components that are used only for specific deployments, depending on the NAP enforcement method or methods chosen by the IT staff.

NAP enforcement methods are any of 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.

#### Common NAP components

Common NAP components consist of both client and server components. A NAP-capable client is a computer that has the NAP components installed and that can verify its health state by sending a list of Statements of Health to Network Policy Server.

#### Common client components

The common NAP client components are:

* System Health Agent (SHA)—System Health Agents (SHAs) monitor and report the client computer's state of compliance, so that NPS can determine whether the settings monitored by the SHA are up to date and configured correctly. For example, the Microsoft SHA can monitor to see if Windows Firewall is enabled, and whether antivirus software is installed, enabled, and updated. There might also be SHAs available from other companies that provide additional functionality.
* Statement of Health (SoH)—A Statement of Health is a declaration from a system health agent that asserts its health status. System health agents create statements of health and send them to the NAP Agent.
* NAP agent—NAP agent collects and manages health information. NAP agent also processes Statements of Health from SHAs and reports client health to installed enforcement clients. To indicate the overall health state of a NAP client, the NAP Agent uses a list of SoHs.
* NAP enforcement client (NAP EC)—To use NAP, at least one NAP enforcement client must be installed and enabled on client computers. Individual NAP enforcement clients are enforcement method-specific. The NAP enforcement client requests access to a network, communicates a client computer's health status to the NPS server, and communicates the restricted status of the client computer to other components of the NAP client architecture.

#### Common server components

The common NAP server components are:

* Health policies—NPS policies define health requirements and enforcement settings for client computers requesting network access. NPS processes RADIUS Access-Request messages containing the list of SoHs sent by the NAP enforcement client, and passes them to the NAP Administration server.
* NAP Administration server—The NAP Administration server component provides a processing function that is similar to the NAP Agent on the client side. It receives the list of SoHs from the NAP enforcement server through NPS, and distributes each SoH to the appropriate SHV. It then collects the resulting SoH Responses from SHVs and sends them to NPS for evaluation.
* System Health Validators (SHVs)—SHVs are server software counterparts to SHAs. Each SHA on the client has a corresponding SHV in NPS. SHVs verify the SoH that is made by its corresponding SHA on the client computer.
  + SHAs and SHVs are matched to each other, along with a corresponding policy server (if required) and perhaps a remediation server.
  + An SHV can also detect that no SoH has been received, such as in the case where the SHA has never been installed, or has been damaged or removed. Regardless of whether the SoH meets the defined policy, the SHV sends a Statement of Health Response (SoHR) message to the NAP Administration server.
  + One network might have more than one kind of SHV. If it does, the NPS server must coordinate the output from all of the SHVs and determine whether to limit the access of a noncompliant computer. This requires careful planning when defining health policies for the environment and evaluating how different SHVs interact.
* NAP enforcement server (NAP ES)—The NAP enforcement server is matched to a corresponding NAP EC for the NAP enforcement method being used. It receives the list of SoHs from the NAP EC and passes them to NPS for evaluation. Based on the response, it provides limited, unlimited or no network access to a NAP-capable client. Depending on the type of NAP enforcement, the NAP ES may be a certification authority (IPSec enforcement), an authenticating switch or wireless access point (802.1x enforcement), a Routing and Remote Access Server (VPN enforcement), or a DHCP server (DHCP enforcement).
* Policy server—A policy server is a software component that communicates with an SHV to provide information used in evaluating requirements for system health. For example, a policy server, such as an antivirus signature server, can provide the version of the current signature file for validation of a client antivirus SoH. Policy servers are matched to SHVs, but not all SHVs require a policy server. For example, an SHV can just instruct NAP-capable clients to check local system settings to ensure that a host-based firewall is enabled.
* Remediation server—A remediation server hosts the updates that SHAs can use to bring noncompliant client computers into compliance. For example, a remediation server can host software updates. If health policy requires that NAP client computers have the latest software updates installed, the NAP EC will restrict network access to clients without these updates. Remediation servers must be accessible to clients with restricted network access in order for clients to obtain the updates required to comply with health policies.
* Statement of health response (SoHR)—After the client SoH is evaluated against health policy by the appropriate SHV, a Statement of Health response is generated that contains the results of the evaluation. The SoHR reverses the path of the SoH and is sent back to the client computer SHA. If the client computer is deemed noncompliant, the SoHR contains remediation instructions that the SHA uses to bring the client computer configuration into compliance with health requirements.

Just as each type of SoH contains different kinds of information about system health status, each SoHR message contains information about how to become compliant with health requirements.

### Client computer health

For NAP, health is defined as the information about a client computer that is used to determine whether the client should be allowed unlimited or limited or no access to a network. NAP assesses a client computer's health state and compares it to the state that is required by configured health policies.

Example measurements of health could include:

* Operational status of Windows Firewall—Is the firewall enabled or disabled?
* Update status of antivirus signatures—Are the antivirus signatures the most recent ones available?
* Installation status of security updates—Are the most recent security updates installed on the client?

The client computer's health status is encapsulated in a list of statements of health (SoHs), issued by NAP client components. NAP client components send the list of SoHs to NAP server components for evaluation to determine whether the client is compliant and can be granted unlimited network access.

NAP allows administrators to ensure ongoing compliance with health policies, and to limit the access of noncompliant computers until the health state of those computers can be brought into compliance with health policy. In NAP terminology, verifying that a computer meets an organization’s defined health requirements is called health policy validation. NPS performs health policy validation for NAP.

### **NAP Administration server**

The NAP Administration server component provides a processing function that is similar to the NAP Agent on the client side. It receives the list of SoHs from the NAP enforcement server through NPS, and distributes each SoH to the appropriate SHV. It then collects the resulting SoH Responses from SHVs and sends them to NPS for evaluation.

### Network Policy Server (NPS)

In earlier versions of Windows, the Network Policy Server (NPS) was named Internet Authentication Service (IAS). NPS now provides multiple features, including the ability to act as a NAP policy server for all four NAP enforcement methods: 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.

When users configure NPS as a NAP policy server, NPS evaluates lists of Statements of Health sent by NAP-capable client computers that want to connect to or communicate on the network. IT administrators configure NAP policies in NPS, including System Health Validators (SHVs), SHV templates, and Remediation Server Groups that allow client computers to update their configuration to become compliant with the organization's health requirements.

NPS is also the Microsoft implementation of a Remote Authentication Dial-In User Service (RADIUS) server and proxy. As a RADIUS server, NPS performs centralized connection authentication, authorization, and accounting for many types of network access, including 802.1X wireless and authenticating switch and remote access dial-up and virtual private network (VPN) connections. As a RADIUS proxy, NPS forwards authentication and accounting messages to other RADIUS[[1]](#footnote-2) servers.

### Example: How NAP Enforcement Works

As stated above, NAP enforces health requirements by monitoring and assessing the health of client computers, and limiting network access when client computers are deemed noncompliant. Both client and server components assist in the remediation of noncompliant client computers so that they can obtain unlimited network access. Several key processes are necessary for NAP to function properly:

* Policy validation
* NAP enforcement and network restriction
* Remediation
* Ongoing monitoring to ensure compliance

#### Policy validation

With NPS, administrators can create client health policies using SHVs that allow NAP to detect, enforce, and remediate client computer configurations.

The Windows System Health Agent and Windows System Health Validator enforce the following settings for NAP-capable computers. The client computer has:

* Firewall software installed and enabled
* Antivirus software installed and running
* Current antivirus updates installed
* Antispyware software installed and running
* Current antispyware updates installed
* Microsoft Update Services enabled

In addition, if NAP-capable client computers are running Windows Update Agent and are registered with a Windows Server Update Service (WSUS) server, NAP can verify that the most recent software security updates are installed based on one of four possible values that match security severity ratings from the Microsoft Security Response Center (MSRC). The four severity ratings are:

* Critical—A vulnerability whose exploitation could allow a program of an Internet worm without user action.
* Important—A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users’ data, or of the integrity or availability of processing resources.
* Moderate—Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.
* Low—A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

#### NAP enforcement and network restriction

NAP can be configured to deny noncompliant client computers access to the network or allow them access to only a restricted network. A restricted network should contain key NAP services, such as Health Registration Authority (HRA) servers and remediation servers, so that noncompliant NAP clients can update their configurations to comply with health requirements. NAP enforcement settings allow the IT staff to either limit network access of noncompliant clients, or to observe and log the health status of NAP-capable client computers.

Users can choose to restrict access, defer restriction of access, or allow access by using the following settings:

* Do not enforce—This is the default setting. Clients that match the policy conditions are deemed compliant with network health requirements, and granted unrestricted access to the network if the connection request is authenticated and authorized. The health compliance status of NAP-capable client computers is logged.
* Enforce—Client computers that match the policy conditions are deemed noncompliant with network health requirements, and are placed in the restricted network.
* Defer enforcement—Clients that match the policy conditions are temporarily granted unrestricted access. NAP enforcement is delayed until the specified date and time.

#### Remediation

Noncompliant client computers that are placed on a restricted network might need remediation. Remediation is the process of updating a client computer so that it meets current health requirements. For example, a restricted network might contain a File Transfer Protocol (FTP) server that provides current virus signatures so that noncompliant client computers can update their outdated signatures.

Administrators can use NAP settings in NPS health policies to configure automatic remediation, so that NAP client components automatically attempt to update the client computer when it is noncompliant.

#### Ongoing monitoring to ensure compliance

NAP can enforce health compliance on compliant client computers that are already connected to the network. This functionality is useful for ensuring that a network is protected as health policies change and the health of client computers change. For example, NAP can determine that the client computer is in a noncompliant state if health policy requires that Windows Firewall be turned on, but a user inadvertently has turned it off. NAP will then place the client computer on the restricted network until Windows Firewall is turned back on. If automatic remediation is enabled, NAP client components can automatically enable Windows Firewall without user intervention.

### NAP enforcement methods

NAP enforces health policies for the following network technologies:

* Internet Protocol security (IPSec) protected traffic
* 802.1X port-based wired and wireless network access control
* Virtual private networks (VPN) with Routing and Remote Access
* Dynamic Host Configuration Protocol (DHCP) IPv4 address lease and renewal

The following sections describe these enforcement methods.

#### NAP enforcement for IPSec communications

NAP enforcement for IPSec-protected traffic is deployed with a health certificate server, a Health Registration Authority (HRA) server, an NPS server, and an IPSec enforcement client. When NAP clients are determined to be compliant, the health certificate server issues X.509 certificates. These certificates are then used to authenticate NAP clients when the authenticated client initiates IPSec-protected communications with other NAP clients on an intranet.

IPSec enforcement confines the communication on the network to compliant clients, and provides the strongest form of NAP enforcement. Because this enforcement method uses IPSec, administrators can define requirements for protected communications on a per-IP address or per-TCP/UDP port number basis.

#### NAP enforcement for 802.1X

NAP enforcement for 802.1X port-based network access control is deployed with an NPS server and an Extensible Authentication Protocol Host (EAPHost) enforcement client component. With 802.1X port-based enforcement, an NPS server instructs an 802.1X authenticating switch or an 802.1X compliant wireless access point to place noncompliant 802.1X clients on a restricted network. The NPS server limits the client's network access to the restricted network by instructing the access point to apply IP filters or a virtual LAN identifier to the connection. 802.1X enforcement provides strong network restriction for all computers accessing the network through 802.1X-capable network access devices.

#### NAP enforcement for VPN

NAP enforcement for VPN is deployed with a VPN Enforcement Server component and a VPN enforcement client component. Using NAP enforcement for VPN, VPN servers can enforce health policy when client computers attempt to connect to the network by using a remote access VPN connection. VPN enforcement provides strong ability to limit network access for all computers accessing the network through a remote access VPN connection that don’t meet client health requirements. VPN enforcement is different from Network Access Quarantine Control, which is a feature in Windows Server 2003 and Internet Security and Acceleration (ISA) Server 2004.

#### NAP enforcement for DHCP

DHCP enforcement is deployed with a DHCP NAP enforcement server component, a DHCP enforcement client component, and NPS. Using DHCP enforcement, DHCP servers and NPS can enforce health policy when a computer attempts to lease or renew an IP version 4 (IPv4) address. The NPS server limits the client's network access to the restricted network by instructing the DHCP server to assign a limited IP address configuration. However, if client computers are configured with a static IP address or are otherwise configured to circumvent the limited IP address configuration, DHCP enforcement is not effective. Health validation data that is stored in DHCP messages is visible to other computers. The DHCP Enforcement Client sends the list of SoHs only if the DHCP server requests it.

#### Combined approaches

Each of these NAP enforcement methods has different advantages. By combining enforcement methods, administrators can combine the advantages of these different methods. Deploying multiple NAP enforcement methods, however, can make the NAP implementation more complex to manage.

The NAP framework also provides a suite of APIs that allow companies other than Microsoft to integrate their software into the NAP platform. By using the NAP APIs, software developers and vendors can provide end-to-end solutions that validate health and remediate noncompliant clients.

## Summary

With Windows Server 2008, organizations can benefit from improvements in security through policy based security features such as Network Access Protection. Security related improvements in Active Directory such as RODC, and new auditing options, combined with improvements in Enterprise PKI make it easier for administrators to secure the organization, and audit security events, even in remote locations. Other features of the operating system such as Windows BitLocker Drive Encryption and new Windows Firewall features make it a more secure out-of-the-box. Windows Server 2008 is the right choice for organizations that want a more secure server platform and network environment. The identity and access features in Windows Server 2008 combine with the improved Federated Rights Management capabilities to simplify the ability to manage user identities and access privileges and share sensitive content with external users.

# Chapter 6: Web & Applications

## Introduction

Microsoft Windows Server 2008 provides a secure, easy-to-manage platform for developing and reliably hosting applications and services from the server or over the Web. New features include: simplified application and services management, quicker deployment, increased security, and improvements to both performance and extensibility. Windows Server 2008 provides these improvements, while allowing administrators fine control and visibility into how applications and services are utilizing key operating system resources. Key benefits include:

* Deliver rich Web-based experiences efficiently and effectively
* Reduced Web server attack surface, footprint, and patching through modular architecture and fully customizable installation
* Greater reliability and security of Web sites and applications through automatic sandboxing of new Web sites
* XCopy deployment along with *c*ode and content by leveraging new distributed configuration system
* Easier administration with powerful new administration tools
* Improved diagnostic and troubleshooting tools that minimize downtime and speed up failure recovery
* Integrated .NET Framework 3.0 including support for
  + Windows Communication Foundation (WCF)
  + Windows Presentation Foundation (WPF)
  + Windows Workflow Foundation (WF)
  + Windows CardSpace (WCS)
* Integrated PHP support for running common non-Microsoft Web applications
* An industrial-strength platform for streaming live or on-demand audio and video content over the Internet or an intranet
* Collaboration technology and Web-based application platform designed to improve business processes and enhance team productivity

## Internet Information Services (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. Key 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 administrative model for Web solutions.

### Modular Design

The IIS 7.0 core Web server includes some fundamental changes from IIS 6.0. In previous versions of IIS, all functionality was built-in. 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 need to be managed and updated.

There are also processing changes. Both native and managed code is processed through a single request pipeline. The new worker process Web core also provides access to all notification events in the request pipeline. The level of integration allows existing ASP.NET features (such as Forms-based authentication or URL authorization) to be used for all types of Web content.

These changes enable a significant reduction in attack surface because no unnecessary software is running, more extensibility, and increased support for extending IIS 7.0 core functionality by creating managed code modules.

### Increased Extensibility

In previous versions, extending or replacing built-in functionality of the core Web server presented some challenges. With IIS 7.0, developers can create managed code modules that extend functionality, for example a custom authentication set created in .Net. IIS 7.0 uses 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, although 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, administrators and developers have the flexibility to add, remove, or even replace IIS feature modules if they like.

Modules may be developed in both native code (C/C++) and managed code (languages, such as C#, and Visual Basic® 2005, that use the .NET Framework). The IIS 7.0 integrated request processing pipeline is also able to provide notifications to managed code Modules (IHttpModule) and Handlers (IHttpHandler), enabling managed code modules to access all events in the request pipeline, for all requests in the pipeline. This provides greater control of all events in the pipeline by managed code modules and handlers that filter client requests and manipulate URLs by implementing the IHttpModule interface or the IHttpHandler interface. 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.

### Distributed Configuration

IIS 7.0 introduces major improvements to the way its configuration data is stored and accessed through distributed configuration of the IIS settings. This enables administrators to specify IIS configuration settings in files that are stored with the code and content. By specifying configuration settings in a single file, is it now possible to delegate administration responsibilities of selected Web site features or Web applications to others, and to use simple XCopy deployments.

#### Changes that Allow Distributed Configuration

The centralized configuration store of IIS 6.x, known as the metabase, is gone. IIS 7.0 features a new delegated configuration system based on a hierarchy of distributed XML configuration files. This hierarchy is comprised of a global applicationHost.config file, which contains server-level configuration defaults, and distributed Web.config files within the application's directory structure. These are the same Web.config files that are used by the ASP.NET application framework to store application settings in a portable way. This allows the side-by-side storage of IIS and ASP.NET configuration, using clean and strongly structured XML directives. This change provides one configuration store for all Web platform configuration settings that are accessible via a common set of APIs and stored in a consistent format. The IIS 7.0 configuration system is also fully extensible, so developers can extend the configuration store to include custom configuration with the same fidelity and priority as IIS configuration.

In the past, IIS application settings had to be explicitly configured in the machine-level metabase repository before the application could function correctly. With distributed Web.config files, applications encapsulate the required server configuration within their directory structure. This dramatically simplifies deployment, allowing self-contained applications to be simply copied to the target server's application directory and thus be up and running immediately with the desired settings.

IIS 7.0 stores the ApplicationHost.config in the %windir%\system32\inetsrv directory . In this file there are two major configuration section groups:

* system.applicationHost
* system.WebServer

The system.applicationHost section group contains configuration for site, application, virtual directory and application pools. The system.WebServer section group contains configuration for all other settings, including global Web defaults.

#### XCopy Deployment

Distributed configuration 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 avoid costly and error-prone replication, manual synchronization, and additional configuration tasks. This makes it easier to copy the configuration settings for a specific site or application one computer to another as the application moves from development into test, and ultimately into production. XCopy deployment means that the application developer can make configuration changes to their application, without involving the machine administrator—which translates to overall lower TCO. Easy XCopy deployment also means that the machine administrator can easily move sites across machines.

### Administration Tools

IIS 7.0 introduces the following updated and revised administration tools for managing IIS:

* + IIS Manager, with the new graphical administration interface
  + Command line scripts have been replaced with a powerful new command-line tool, appcmd.exe
  + Configuration store, based on the .NET Framework 2.0 configuration store, which supports the direct editing of settings
  + WMI Provider is a software component that functions as mediator between the CIM Object Manager and managed objects. It provides access to configuration and server state information to Visual Basic Scripting Edition (VBScript) and JScript writers.
  + Managed interface, Microsoft.Web.Administration, which exposes the same information exposed by the WMI provider in a simpler application programming interface (API). Developers can use Microsoft.Web.Administration to control and read all functions in IIS 7.0.

In addition, the IIS 6.0 MMC snap-in is provided with Windows Server 2008 to support remote administration of IIS 6.0 from Windows Server 2008, and to administer FTP sites. IIS 6.0 administration tools and Web server components can be installed separately.

The new administration tools in Windows Server 2008 fully support the new IIS 7.0 distributed configuration, and allow for delegated access to site and application configuration for non administrators (described further in the Delegated Administration section below).

### New IIS Manager

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 IIS Manager interface supports remote administration over HTTP, allowing for integrated local and remote administration, without requiring DCOM or other administrative ports be opened on the firewall.

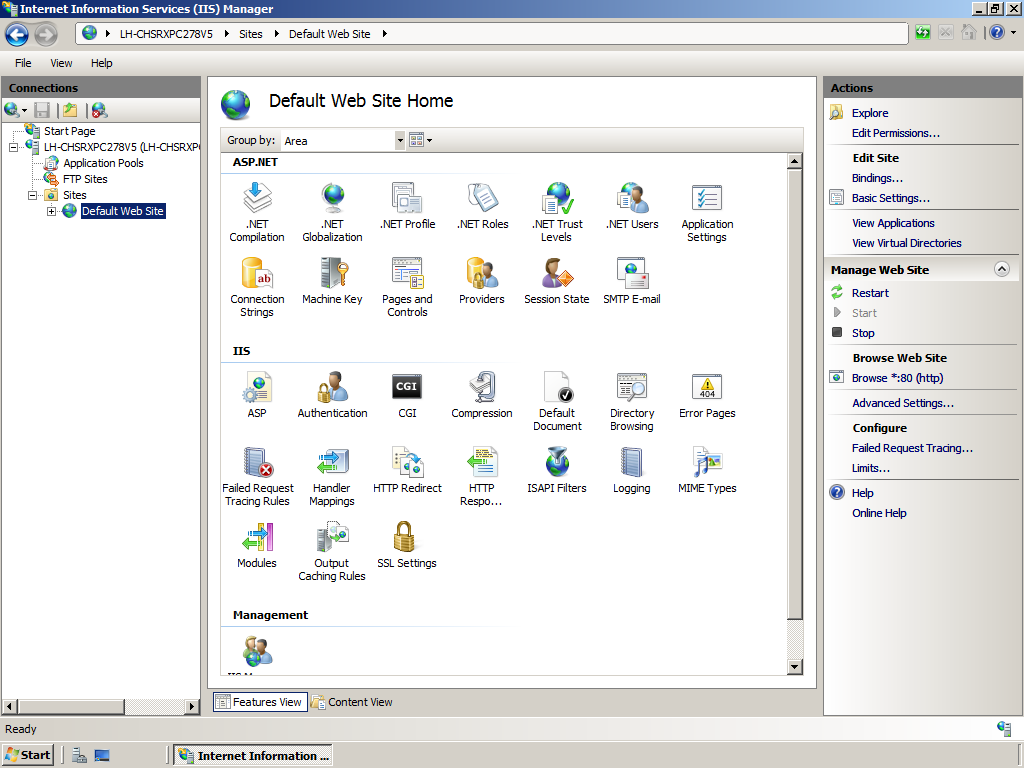


Figure 5: The new IIS administration screen

IIS Manager also allows administrators to delegate administrative control to developers or content owners. Other key features of IIS Manager include:

* + A rich extensibility framework for plugging in new UI features using the .NET Framework
  + Support for both Windows and non-Windows credentials for delegated administration
  + Automatic downloading and installation of new UI modules to the client
  + Remote administration over HTTP/SSL

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 had to wait for more than 500 milliseconds. This information can be used to troubleshoot applications that are performing poorly. The output of appcmd.exe can be piped into other commands for further processing.

#### Delegated Administration

Distributed configuration in IIS 7.0 enables those who host or administer Web sites delegate varying levels of administrative control to developers or content owners, thus helping to reduce the cost of ownership and the workload for the administrator. For example, the administrative control of a Web site might be delegated so that the application developer can configure and maintain the default document or other properties 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. The delegation can be very specific, allowing an administrator to decide exactly which functions to delegate, on a case-by-case basis.

#### Microsoft.Web.Administration

IIS 7.0 also includes Microsoft.Web.Administration, a new management API for the Web server that enables editing configuration settings through manipulation of the XML configuration files. It also provides objects to manage the server, server properties, and server state. This API provides programmatic access to read-and-write configuration properties in the IIS configuration file hierarchy and to the same data that has historically been accessible by WMI scripts in the previous versions of IIS.

### Diagnostics and Troubleshooting

IIS 7.0 makes troubleshooting the Web server easier than ever with built-in diagnostics and tracing support, allowing the administrator to see detailed, real-time diagnostic information about a Web server. Diagnostics and troubleshooting features allow a developer or an administrator to see requests that are running on the server, making it possible to filter for error conditions that are difficult to reproduce and automatically trap errors with a detailed trace log.

#### Detailed Error Messages

IIS 7.0 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. The default is localhost, but it can be configured to send error information to other remote clients as well. 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.

#### Runtime Status and Control API (RSCA)

One of the most important features that 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 within IIS 7.0. With RSCA, it is possible to inspect and manage various entities including sites, application pools, .NET Framework application domains and even running requests. This information can be used by administrators or developers to analyze server resource utilization and troubleshoot Web applications.

For example, with RSCA and the IIS 7.0 administration tools, administrators can know what requests are executing in a worker process that's consuming 100% of the CPU, or which application domains are loaded for a particular site. RSCA also surfaces currently executing requests on the server in real time. RSCA data is available from the WMI provider and managed API (Microsoft.Web.Administration). The IIS Manager command-line tool (appcmd.exe) also can display this data.

#### Failed Request Tracing

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 back out 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.

If a request to a server fails or takes too long, the administrator can define a failed request tracing rule that will capture trace events for that request and log these trace events as they occur. Events are written to the trace log if the request exceeds the time interval allocated for the request to complete processing, or if a specified HTTP status and sub-status code combination is generated for the response. Trace log entries can also be triggered by event verbosity levels. The trace log only contains information specific to that failed request. Administrators no longer must search through large log files that contain every request to find the information that they need about a specific failed request. The new XSL sheet is designed to help present the data in different cross-sectional views to aid in diagnosing the various problems that Web applications could encounter.

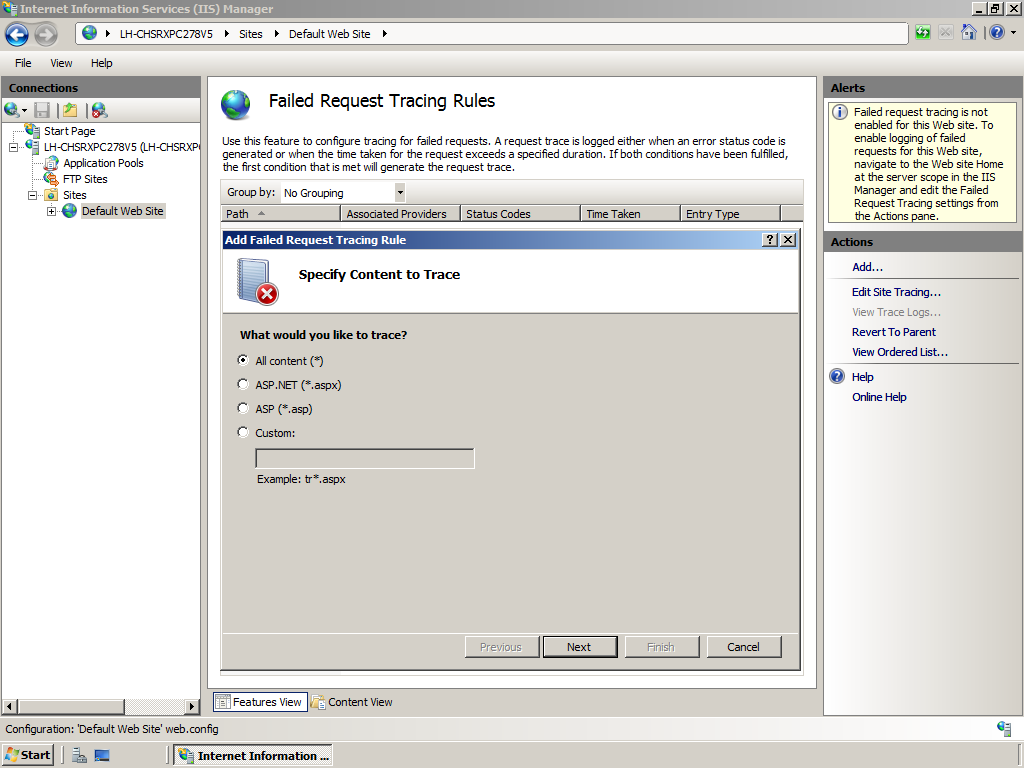


Figure 6: The Failed Request Tracing Rules screen

## Windows Process Activation Service (WAS)

To enhance the development and hosting of Windows Communication Foundation (WCF) services over many protocols (see “Windows Communication Foundation (WCF),” below), Windows Server 2008 includes the Windows Process Activation Service (WAS), which supports pluggable activation of arbitrary protocol listeners. WAS provides all types of message-activated applications with intelligent resource management, on-demand process activation, health monitoring, and automatic failure detection and recycling. WAS is based on the IIS 6.0 request processing model.

WAS uses application pool configuration and worker processes instead of WWW Service, enabling applications to use the same configuration and process models for HTTP and non-HTTP sites. By running independent of WWW Service, WAS can manage Web services through listeners such as NET.TCP. This is useful for applications that do not need to listen for HTTP requests in HTTP.sys.

## Windows System Resource Manager (WSRM)

Windows System Resource Manager enables administrators to control how CPU and memory resources are allocated to applications, services, and processes. Managing resources in this way improves system performance and reduces the chance that applications, services, or processes will interfere with the rest of the system. It also creates a more consistent and predictable experience for users of applications and services running on the computer.

WSRM integrates resource management with Web pools and sessions through built-in policies including Equal\_Per\_IISAppPool and Equal\_Per\_Session.Conditional. Policies in WSRM automatically switch to different resource allocations in response hardware hot-add changes or cluster changes if running in a cluster configuration.

WSRM also features many new accounting additions. With SQL Server 2005, administrators can capture resource usage statistics in a standard format that can be fed into chargeback and other cost-based models using the SQL-based account engine (on x86-based and x64-based servers only). Moreover, WSRM provides support for storing accounting data from multiple WSRM-managed machines into a single consolidated database (as opposed to having to build a front-end, Web-based tool to collect data from multiple servers for chargeback and accounting). WSRM also directly supports storing accounting data in SQL Server 2005 databases.

All previous versions of WSRM were distributed on a separate WSRM CD and required a separate installation step. With Windows Server 2008, that has changed: now WSRM resides on the installation medium and may be installed or removed like any other built-in optional component through the Optional Component dialog box. WSRM is available in all editions of Windows Server 2008 and it will run on any computer that supports Windows Server 2008.

## Eventing Infrastructure

### **Events in Windows Server 2008 and Windows Vista**

Windows Server 2008 has a new eventing architecture that overcomes some challenges with eventing and tracing in previous versions. The challenges addressed include limited scalability of the Event Log (which limited the total size of all logs to the amount of available memory), event publishing performance (which, for example, limited the number of events that could be published on an active Domain Controller), and limited security of the trace events.

Eventing 6.0 replaces the Event Log service and the Event Viewer. Windows Eventing is designed to deal specifically with events that are persisted into log files for future examination. It is not intended for transient events like IPC and notification mechanisms.

### **New Ways to View Events**

The new Event Viewer has been completely rewritten and, because it works within the Microsoft Management Console (MMC) 3.0, its appearance has also changed. As with previous versions, there is a tree pane and a list of events. The familiar Application, System, and Security logs under the Windows Logs node are still accessible. Some new nodes have also been added. There is a preview pane, located under the event list. It contains the properties of the focused event. Events can be collected for one or more log files, and can focus on specific IDs, severity levels, or time frames. With the new interface, administrators no longer have to double-click an event to see the event properties, and don't have to juggle windows in order to see both the list and the Event Properties dialog box.

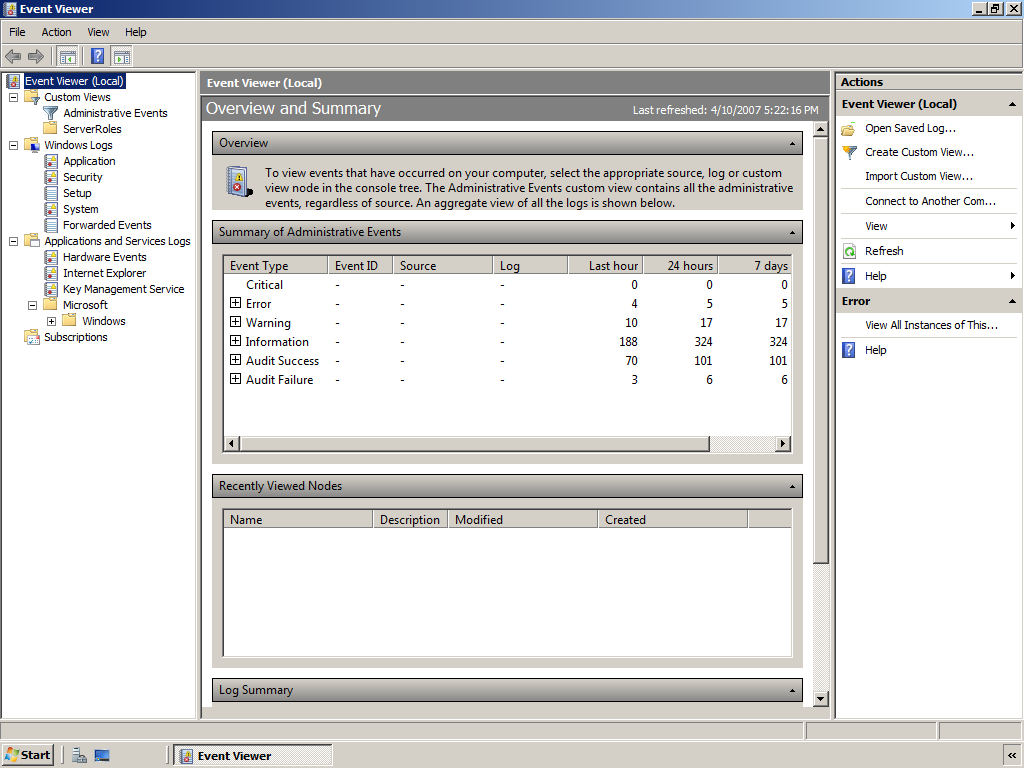


Figure 7: The new Event Viewer screen

### **XML Structure**

The new Event logs follow a well-defined structure. Events are represented externally using XML with a published schema. This makes it possible to create queries that collect the events of interest while filtering out extraneous events. Internally the events are saved in a binary format that is designed to provide a balance of compactness, reliability, and search performance.

Since XML is used, XPath is the base for the event query language. The use of structured events allows new opportunities for automation, as can been seen with the new Task Scheduler integration. A simple XPath expression (supplied to the Event log command-line utility) can be used to select events from a single log, a simple but powerful XML-based query language allows selection and suppression of events from any log or external event archive.

### **Event Subscriptions**

While the Event Viewer allows administrators to view events on a single local or remote computer, troubleshooting an issue might require examination of a set of events stored in multiple logs on multiple computers. Windows Server 2008 and Windows Vista include the ability to collect copies of events from multiple remote computers and store them locally. To specify which events to collect, administrators create an event subscription. Among other details, the subscription specifies exactly which events will be collected and in which log they will be stored locally. Once a subscription is active and events are being collected, the forwarded events can be manipulated like any other locally stored events.

The new Eventing features in Windows Server 2008 make it easier for server and applications administrators to monitor their applications, collect logged data for analysis, and troubleshoot issues that arise.

## The Restart Manager

The Restart Manager API in Windows Server 2008 can eliminate or reduce the number of system restarts that are required to complete an installation or update. The Restart Manager shuts down and restarts all but the critical system services, and unloads blocking DLLs and resources. This frees files that are in use and allows installation operations to complete.

The update of any file or resource owned by a critical system service, by the Windows Installer, the Window Update Agent, or Windows Management Instrumentation (WMI) requires a system restart. Critical system services include smss.exe, csrss.exe, winit.exe, logonui.exe, lsass.exe, services.exe, winlogon.exe, csrss.exe, svchost.exe with RPCSS, and svchost.exe with Dcom/PnP.

The Restart Manager stops applications in the following order:

1. GUI applications
2. Console applications
3. Windows services
4. Windows Explorer

The Restart Manager restarts the applications that have been registered for restart in the reverse order in which they were stopped.

The Restart Manager DLL exports a public C interface that can be loaded by standard or custom installers. During the installation of an application or update, the installer can use the Restart Manager to determine which files cannot be updated because they are currently in use. Restart Manager can shut down and restart the non-critical services or applications that are currently using those files.

Developers can write installers that direct the Restart Manager to shut down and restart applications or services based on the:

* + file in use
  + process ID (PID)
  + short name of a Windows service

Files that are found to be in use, that cannot simply be deleted and replaced by an update, can be registered with the Restart Manager. The applications or services that are using those files can then be safely shut down and restarted.

Minimizing restarts interrupts applications less and increasing system uptime.

## Microsoft .NET Framework 3.0

The Microsoft .NET Framework version 3.0 (formerly WinFX®) is the managed-code programming model for Windows. It includes version 2.0 of the Common Language Runtime and 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.

Additions in the .NET Framework 3.0 include:

* Windows Communication Foundation (WCF)
* Windows Presentation Foundation (WPF)
* Windows Workflow Foundation (WF)
* Windows CardSpace (WCS), formerly known as InfoCard

Microsoft .NET Framework 3.0 is included as part of the Application Server role in Windows Server 2008 and as part of Windows Vista. It is also available for Windows XP Service Pack 2 and Windows Server 2003 Service Pack 1.

Microsoft .NET Framework 3.0 is a superset of the .NET Framework 2.0, and is an additive release to the .NET Framework 2.0. This is contrasted with a generational release, where software is revised. Microsoft .NET Framework 3.0 uses the core run-time components from the previous .NET Framework, and it is backward-compatible with applications created in the .NET Framework 2.0.

### Windows Communication Foundation (WCF)

Windows Communication Foundation (WCF) is a set of .NET Framework technologies for building and running connected systems. WCF unifies and extends the functionality of existing Microsoft connecting technologies, providing a single programming model independent of underlying communications protocols. WCF applications can interoperate with other technologies using open standards and protocols. Advanced Web services support in Windows Communication Foundation provides secure, reliable, and transacted messaging along with interoperability. The service-oriented programming model of Windows Communication Foundation, built on Microsoft .NET Framework, simplifies development of connected systems. Windows Communication Foundation is available for Windows Server 2008 and Windows Vista, as well as for Windows XP and Windows Server Windows Server 2003.

Windows Communication Foundation represents the next generation connecting technology that combines and extends the best attributes of existing connecting technologies to deliver a unified development and runtime experience. It provides a single API and a consistent, straightforward programming model that supersedes the following technologies:

* DCOM and .NET Remoting support for efficient Remote Procedure Call (RPC) functionality
* ASP.NET Web Services (ASMX) support for easily configurable, interoperable Web Services
* .NET Framework Enterprise Services support for synchronization, distributed transactions, basic security, and distributed COM+ Services
* Web Services Enhancements (WSE) support for open Web Service standards, collectively known as WS-\* specifications including security, reliable messaging, and distributed transactions specifications
* Queued messaging that is compatible with either MSMQ or the .NET Framework System.Messaging namespace technologies

IIS 7.0 includes new management interfaces to view, filter, and troubleshoot messages from WCF and to manage IIS settings, user data, and diagnostics.

### Windows Presentation Foundation (WPF)

WPF provides the foundation for building applications and high fidelity experiences in Windows Vista and Windows Server 2008, blending together application UI, documents, and media content, while exploiting the full power of the computer. The functionality extends to the support for Tablet and other forms of input, a more modern imaging and printing pipeline, accessibility and UI automation infrastructure, data driven UI and visualization, as well as the integration points for weaving the application experience into the Windows shell.

### Windows Workflow Foundation (WF)

Windows Workflow Foundation is the programming model, engine, and tools for quickly building workflow enabled applications on Windows. It consists of an in-process workflow engine, an API, and designers for Visual Studio® 2005. Windows Workflow Foundation is available for both client and server versions of Windows. Windows Workflow Foundation includes support for both system workflow and human workflow across a wide range of scenarios including; workflow within line of business applications, user interface page-flow, document-centric workflow, human workflow, composite workflow for service oriented applications, business rule driven workflow and workflow for systems management.

### Windows CardSpace

Windows CardSpace™ is a new feature of Microsoft Windows that helps users better manage and more safely control the exchange of their digital identities. It provides an environment that protects users and their sensitive data from common phishing and fraud attacks and helps users make safer decisions about who they exchange their digital identity information with. Windows CardSpace™ is delivered as part of the .NET Framework 3.0, which is also built-in to Windows Vista and is available as a download for Windows XP and Windows Server 2003.

### Service Trace Viewer Tool (SvcTraceViewer.exe)

Windows Communication Foundation (WCF) Service Trace Viewer Tool helps administrators analyze diagnostic traces that are generated by WCF. Service Trace Viewer provides a way to easily merge, view, and filter trace messages in the log so that users can diagnose, repair, and verify WCF service issues. Diagnostic traces provide information that shows what is happening throughout an application's operation, and can follow operations from their source to destination and through intermediate points too.

## PHP Support

PHP is an open source scripting language that is used by a large number of Web developers. Windows Server 2008 contains functionality that supports running the PHP scripting language on the operating system allowing PHP based Web sites and applications to be hosted on IIS 7.0 Web servers.

IIS 7.0 also includes the FastCGI feature module. FastCGI is a language-independent, scalable, open-extension to CGI that provides high performance. The FastCGI extension is built into Server Core and enables application frameworks such as PHP to achieve improved performance and stability on IIS 7.0. By supporting ASP, ASP.NET, XML, and PHP, IIS 7.0 provides organizations with the flexibility to write applications in the language they prefer, and to host applications on the platform that best suits their needs.

## Certificate Services

Certificate Services provides robust and customizable services for issuing and managing certificates used in many instances to provide authentication and secure access to applications. Windows Vista and Windows Server 2008 introduce new functionality for Certificate Services, including a new COM enrollment control, a new enrollment DLL, and the introduction of Simple Certificate Enrollment Protocol (SCEP), a public key infrastructure (PKI) communication protocol. These changes and enhancements are covered in detail in Chapter 5: Security and Compliance.

## 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 Windows Media servers to deliver content to clients.

Windows Media Services provides the ultimate fast-streaming experience, dynamic programming for on-the-fly and 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 update digital media content on-the-fly.
* 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 services for Windows Media Services that are 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 misbehaving 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, making Windows Server 2008 the best choice for hosting Web and server applications today. The features of .NET 3.0 and integrated capabilities of Windows Communication Foundation (WCF), Windows Presentation Foundation (WPF), Windows Workflow Foundation (WF) and Windows CardSpace make Windows Server 2008 a rich and robust application development and support platform for building Web and server applications. Windows Media Services is a versatile platform for streaming live or on-demand audio and video content over the Internet and an intranet.

# Chapter 7: Server Management

## Introduction

Windows Server 2008 provides a variety of tools, technologies, and installation options to improve managing single and multiple servers across an enterprise. For administering a single server, Server Manager is a unified Microsoft Management Console (MMC) that offers IT Professionals an integrated experience for adding, removing, and configuring server roles, role services, and features. It also acts as a portal for ongoing server management, monitoring, and operations, by exposing key management tasks based on server role, and providing access to advanced administration tools.

Management of multiple servers can be automated using Windows PowerShell, which has a new command-line shell and scripting language designed specifically to automate administration tasks for server roles, such as Internet Information Services (IIS), Terminal Server, and Active Directory, but still preserves existing script investments.

The Windows Remote Shell tool allows IT Professionals to remotely manage servers or to obtain management data through Windows Remote Management (WinRM) and Windows Management Instrumentation (WMI) objects on remote servers. Windows Remote Management is a new remote access protocol that is the Microsoft implementation of the Distributed Manager Task Force (DMTF) standard Web Services for Management (WS-Management).

Server Core is a new feature of Windows Server 2008 that provides a minimal installation option for certain server roles, offering a smaller server footprint and attack surface to reduce management and maintenance needs. This chapter will provide an introduction to these tools and technologies and explain how they improve manageability of Windows Server 2008.

Windows Deployment Services (WDS) is a suite of components that save time by simplify the deployment of Windows operating systems by supporting network-based installation.

## Initial Configuration Tasks

Setting up of Windows Server 2008 is streamlined because the installation process is no longer interrupted by configuration tasks that require user intervention, such as network configuration. Those tasks and dialog boxes now occur after the primary installation has completed, freeing the administrator from having to sit and interact with the installation sequence.

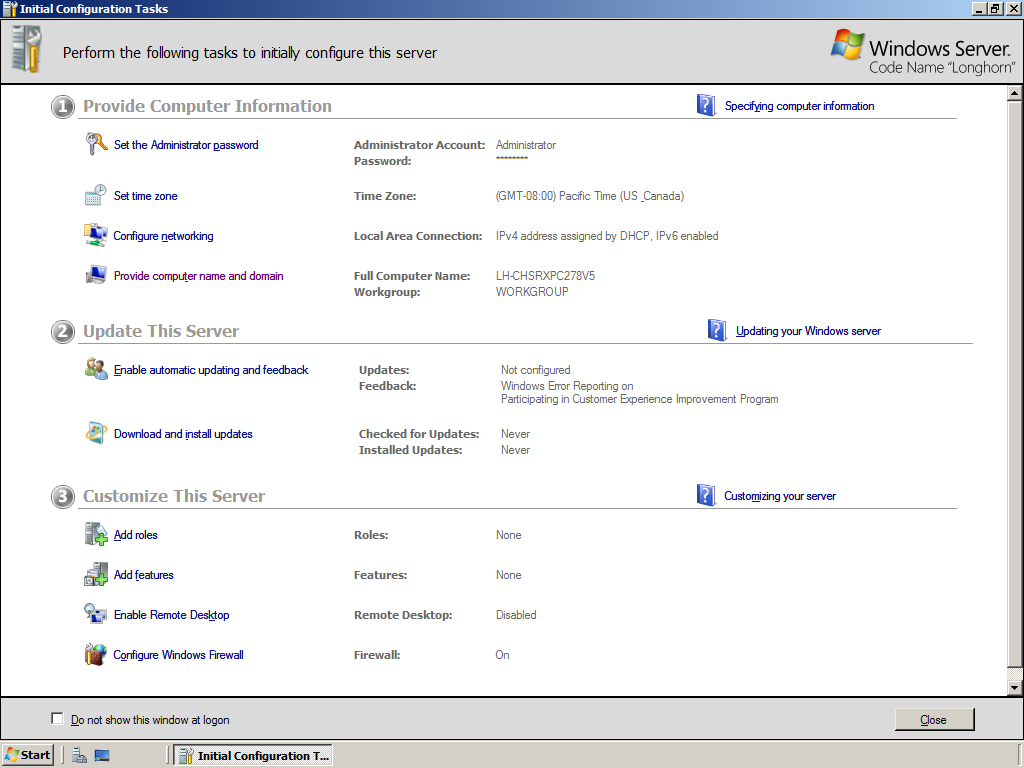


Figure 8: The Initial Configuration Tasks window

The Initial Configuration Tasks window is a new feature in Windows Server 2008 that helps an administrator 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.

#### Default settings in an initial configuration

The following table shows some of the default settings that are configured by the Windows Server 2008 installation process. Commands available in the Initial Configuration Tasks window allow administrators to modify these defaults.

Table 11: AD DS Initial configuration default settings

|  |  |
| --- | --- |
| **Setting** | **Default Configuration** |
| Administrator password | The Administrator account password is blank by default. |
| Computer name | The computer name is randomly assigned during installation. Administrators can modify the computer name by using commands in the Initial Configuration Tasks window. |
| Domain membership | The computer is not joined to a domain by default; it is joined to a workgroup named WORKGROUP. |
| Windows Update | Windows Update is turned off by default. |
| Network connections | All network connections are set to obtain IP addresses automatically by using DHCP. |
| Windows Firewall | Windows Firewall is turned on by default. |
| Roles installed | No role or features are installed by default. |

#### Benefits of Initial Configuration Tasks

The Initial Configuration Taskswindow helps administrators configure a server and shorten the amount of time between operating system installation and deployment of the server in the enterprise. It allows administrators to specify, in a logical manner, operating system settings that were previously configured in Windows Server 2003 Setup, such as the administrator account, domain information, and network settings.

Prior to Windows Server 2008, Windows Server-class operating system setup paused for administrators to provide administrator account, domain, and network information. Customer feedback indicated that this process delayed operating system and server deployment. The Initial Configuration Tasks window allows administrators to postpone these tasks until installation is complete, meaning fewer interruptions and resulting in faster overall deployment.

## Server Manager Console

Windows Server 2008 eases the task of installing, managing, and securing multiple server roles in an organization with the new Server Manager Console. 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 Server Manager Console provides a single, unified console for:

* Managing a server’s configuration and system information
* Displaying server status
* Identifying problems with server role configuration

### Managing the roles, role services and features installed on the server

Roles and features installed by using Server Manager are secure by default. Administrators need not run the Security Configuration Wizard following role installation or removal unless they want to change default settings.

### What are server roles and role services?

A server role describes the primary function of a server. Administrators may choose to dedicate an entire server to one role, or to install multiple server roles on a single computer. Each role may include one or more role services, or optionally installable elements of the role. The following roles are available in Windows Server 2008 and can be installed and managed by using Server Manager:

* Active Directory Certificate Services
* Active Directory Domain Services
* Active Directory Federation Services
* Active Directory Lightweight Directory Services
* Active Directory Rights Management Services
* Application Server
* DHCP Server
* DNS Server
* Fax Server
* File Services
* Network Policy and Access Services
* Print Services
* Terminal Services
* Universal Description, Discovery, and Integration (UDDI) Services
* Web Server (IIS)
* Windows Deployment Services
* Windows SharePoint Services

### What are features?

A feature does not generally describe the primary function of the server. Instead, it describes an auxiliary or supporting function of a server. Consequently, an administrator typically installs a feature not as the primary function of the server, but to augment the functionality of an installed role. For example, Failover Clustering is a feature that administrators can choose to install after installing specific roles, such as File Server, to make the File Server role more redundant. The following features are available in Windows Server 2008 and can be installed by using Server Manager:

* BitLocker Drive Encryption
* BITS Server Extensions
* Connection Manager Administration Kit
* Desktop Experience
* Failover Clustering
* Group Policy Management Console
* Internet Printing Client
* Internet Storage Name Server (iSNS)
* LPR Port Monitor
* Message Queuing
* Microsoft .NET Framework 3.0 Features
* Multipath I/O
* Network Load Balancing
* Peer Name Resolution Protocol
* Quality Windows Audio Video Experience (qWave)
* Recovery Disc
* Remote Assistance
* Remote Server Administration Tools
* Removable Storage Manager
* RPC Over HTTP Proxy
* Services for NFS
* Simple TCP/IP Services
* SMTP Server
* SNMP Services
* Storage Manager for SANs
* Subsystem for UNIX-based Applications
* Telnet Client
* Telnet Server
* TFTP Client
* Windows Internal Database
* Windows Internet Naming Service (WINS)
* Windows PowerShell
* Windows Process Activation Service
* Windows Server Backup
* Windows System Resource Manager
* Wireless Networking

The hierarchy pane of the Server Manager console contains expandable nodes that administrators can use to open consoles for managing specific roles, launch troubleshooting tools, or find backup and disaster recovery options. 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.

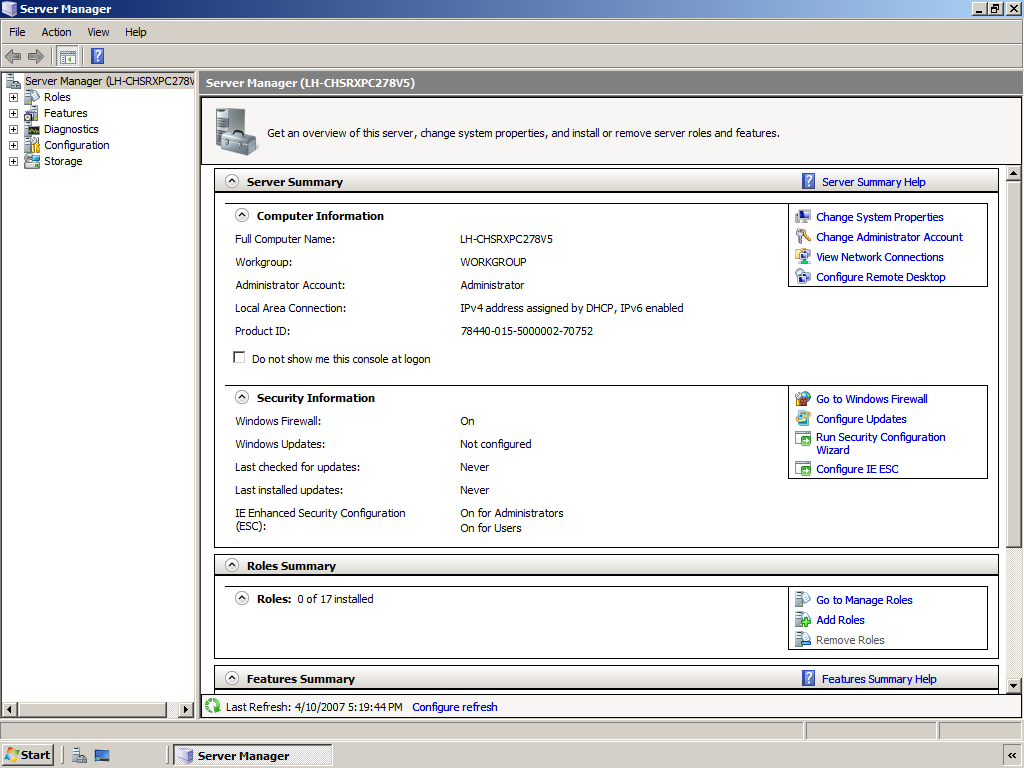


Figure 9: Server Manager main window

The main window of the Server Manager console contains the following four collapsible sections:

* Server Summary—Server Summary includes two subsections; System Information and Security Summary**.** System Information displays the computer name, domain, local administrator account name, network connections, and the product ID of the operating system. Commands in the System Information subsection allow the user to edit this information.
* Security Summary—Security Summary displays the Windows Update and Windows Firewall status. It also displays when the computer was last checked for updates, and when the updates were installed. Commands in the Security Summary subsection allow the administrator to edit these settings or view advanced options.
* Roles Summary—Roles Summary contains a table indicating which roles are installed on the server. Commands in this section allow the administrator to add or remove roles, or open a console from which they can manage a specific role.
* Features Summary—Features Summary displays a table indicating which features are installed on the server. Commands in this section allow features (like BitLocker, Windows Backup, SMTP, etc.) to be added or removed.
* Resources and Support—Resources and Support shows how this server is participating in the feedback programs Windows Server Customer Experience Improvement Program (CEIP) and Windows Error Reporting. CEIP was created to give all Microsoft customers the ability to contribute to the design and development of Microsoft products. CEIP collects information about how customers use Microsoft products and about the problems they encounter. The Resources and Support section is also designed to be a launch point for joining topical newsgroups, or for locating additional help and research topics. It is available online at the Windows Server TechCenter: <http://go.microsoft.com/fwlink/?LinkID=50945>.

The Server Manager Console’s unified management interface in Windows Server 2008 simplifies the management of server configuration and the installed roles.

### Server Manager Wizards

Wizards in Server Manager streamline server deployment tasks in an enterprise by cutting deployment time, compared with earlier versions of Windows Server. 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 that are required by other roles or role services are removed. Windows Server 2008 includes the following role wizards:

#### Add Roles Wizard

For the first time, the Add Roles Wizard can be used to add multiple roles to the server at one time. It automatically checks for dependencies between roles, and verifies that all required roles and role services are installed for each selected role. For some roles, such as Terminal Services and Active Directory Certificate Services (AD CS), the Add Roles Wizard also provides configuration pages that allow the user to specify how the role should be configured as part of the installation process.



Figure 10: Select Server Roles page of the Add Roles Wizard

#### Add Role Services Wizard

Most roles, such as File Services, Terminal Services, and Active Directory Certificate Services, are composed of multiple sub-elements, identified as role services in the Server Manager interface. After one of these complex roles is installed, the administrator can add role services to the role by using the Add Role Services Wizard. The command that opens the Add Role Services Wizard is found on each role home page in the Server Manager console.

#### Add Features Wizard

The Add Features Wizard allows the user to install one or more features to the computer in a single session. Features are software programs that support or augment the functionality of one or more roles, or enhance the functionality of the server itself, regardless of which roles are installed. An example of a feature is Windows PowerShell. Commands that open the Add Features Wizard are in the Customize this serverarea of the Initial Configuration Tasks window, and are also in the Features Summary section of the Server Manager Console window.

#### Remove Roles Wizard

The Remove Roles Wizard can be used to remove one or more roles from the server. It automatically checks for dependencies between roles and verifies that required roles and role services remain installed for roles should not be removed. The Remove Roles Wizard process prevents the accidental removal of roles or role services required by remaining roles on the server.

#### Remove Role Services Wizard

Role Services can be removed from an installed role by using the Remove Role Services Wizard. The command that opens the Remove Role Services Wizard is found on each role home page in the Server Manager console.

#### Remove Features Wizard

The Remove Features Wizard allows administrators to remove one or more features from the computer in a single session. Commands that open the Remove Features Wizard are in the Customize this serverarea of the Initial Configuration Tasks window, and also in the Features Summary section of the Server Manager console.

#### Streamlined installations

Wizards in Server Manager streamline the task of deploying servers in an enterprise by reducing the time required install, configure, or remove roles, role services, and features. Earlier versions of Windows Server required the user to add or remove server roles or other software by means of Configure Your Server, Manage Your Server, or Add or Remove Windows Components. Dependency checks were limited, and Add or Remove Windows Components limited administrators to the installation of only one role at a time. Before more roles could be added, installation of each role had to complete.

The Server Manager collection of wizards allows administrators to add, remove, or augment multiple roles in a single session. It is possible to have the server completely ready for deployment at the completion of a single session in one of the Server Manager wizards. Role configurations are configured with recommended security settings by default; there is no requirement to run the Security Configuration Wizard following role or feature installation unless it is necessary to modify security defaults.

### Server Manager Command-Line Tools

Server Manager offers a command-line tool, ServerManagerCmd.exe, which automates deploying roles and features on computers running Windows Server 2008. The command-line tool can be used to install and remove roles, role services, and features. ServerManagerCmd.exe parameters can also display a list of all roles, role services, and features both installed and available for installation on the computer. The Server Manager command-line interface installation accepts parameters to install or remove one role, role service, or feature per command instance. ServerManagerCmd.exe can be used with an XML answer file to expedite repetitive automated installations or to add or remove multiple of roles or features.

## Windows PowerShell

The Microsoft 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 manage 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 server management and administration tasks as well as the deployment of server roles, such as Terminal Server.

### Consistency and Ease of Use

Managing systems can be a complex endeavor, and tools that have a consistent interface help to control the inherent complexity of the process. The consistency of Windows PowerShell’s commands and syntax is one of its primary assets, reducing the time need to complete administrative tasks and write scripts.

All commands follow standard naming conventions and work with a small set of intuitive utilities (such as -sort, -where, and -list.) to make PowerShell operations more efficient. All commands and the PowerShell scripting language follow an easy to understand verb-noun syntax (for example, get-eventlog; stop=process) that is focused on system administration. Additionally, Windows PowerShell provides simplified navigation of system management stores including the ability to navigate system data, such as the registry and certificate store, as if they were a file system (for example, dir //HKLB; cd \\HKJLM.)

### Interactive and Scripting Environments

Windows PowerShell integrates the command-line shell and scripting language to allow administrators to more efficiently complete and automate system administration tasks. Windows PowerShell improves upon the Windows Command Prompt and Windows Script Host (WSH) by providing cmdlets (command-line tools) 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.

PowerShell supports an organization’s existing scripts (for example, .vbs, .bat, .perl) so the organization does not need to migrate 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.

### Object Orientation and .NET Framework

Although users interact with Windows PowerShell by typing commands in text, Windows PowerShell is based on objects, not text. The output of a command is an object. Users can send the output object to another command as its input. As a result, Windows PowerShell introduces a new and powerful command-line paradigm. Easy-to-understand command-line tools and utilities expose the power of Microsoft .NET technology, Web services, and objects, so administrators can more easily control and automate system administration. Windows PowerShell provides new data and object manipulation utilities that provide administrators an improved ability to filter, sort, group, and compare multiple types of system data such as the registry data, WMI data, and service data. For example, PowerShell can retrieve information through WMI about hardware configuration, such as the amount of free disk on computer. Object-based orientation and the .NET Framework make this powerful functionality possible.

## Group Policy Preferences

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

Organizations typically deploy two types of settings: managed and unmanaged. Managed settings are policy settings that are enforced. Users cannot change policy settings. Policy settings reduce support costs by enforcing standard configurations, help prevent productivity loss, and protect an organization’s assets.

Unmanaged settings are preferences. In contrast to policy settings, users can change preferences. By explicitly deploying preferences rather than accepting the default operating system settings, organizations create configurations that are more compatible with the organization’s IT environment and that are specifically tailored to the organization and how its people use their computers. Additionally, deploying some preferences for users is a necessity in locked-down environments where users can’t change many settings. Organizations deploy preferences in a variety of ways, but the most common are default user profiles, registration entry (.reg) files, and logon scripts. Including preferences in Windows images is also common. Most methods used to deploy preferences, however, are decentralized and unwieldy.

In contrast to the more IT-intensive methods for deploying preferences, Group Policy preferences add a centralized system to Group Policy for deploying preferences. It simplifies deployment, reduces configuration errors, and lowers IT costs. Rather than using the steps described earlier to deploy mapped drives, for example, administrators can simply create a Group Policy object and then edit the Drive Maps preference properties.

### Preferences vs. Policy Settings

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, currently in beta and expected to release shortly after Windows Server 2008, includes the updated GPMC.

The most common question about Group Policy preferences is, “How are preferences different from policy settings?” Understanding this concept is crucial to taking full advantage of Group Policy preferences. The following table summarizes the differences between the two.

Table 12: Preferences vs. Settings

|  | **Group Policy Preferences** | **Group Policy Settings** |
| --- | --- | --- |
| **Enforcement** | * Preferences are not enforced * User interface is not disabled * Can be refreshed or applied once | * Settings are enforced * User interface is disabled * Settings are refreshed |
| **Flexibility** | * Easily create preference items for registry settings, files, and so on * Import individual registry settings or entire registry branches from a local or a remote computer | * Adding policy settings requires application support and creating administrative templates * Cannot create policy settings to manage files, folders, and so on |
| **Local Policy** | * Not available in local Group Policy | * Available in local Group Policy |
| **Awareness** | * Supports non-Group Policy-aware applications | * Requires Group Policy-aware applications |
| **Storage** | * Original settings are overwritten * Removing the preference item does not restore the original setting | * Original settings are not changed * Stored in registry Policy branches * Removing the policy setting restores the original settings |
| **Targeting and Filtering** | * Targeting is granular, with a user interface for each type of targeting item * Supports targeting at the individual preference item level | * Filtering is based on Windows Management Instrumentation (WMI) and requires writing WMI queries * Supports filtering at a GPO level |
| **User Interface** | * Provides a familiar, easy-to-use interface for configuring most settings | * Provides an alternative user interface for most policy settings |

The primary difference between preferences and policy settings is enforcement. Group Policy strictly enforces policy settings. First, Group Policy writes those settings to the Policy branches of the registry, and the access control lists (ACLs) on those branches prevent Standard users from changing them.

Group Policy-aware applications or operating system features look for a potentially managed setting. If the policy setting doesn’t exist, it looks for the setting elsewhere in the registry. Second, Group Policy-aware applications and operating system features typically disable the user interface for settings managed by Group Policy, preventing users from changing them. Finally, Group Policy refreshes policy settings at a regular interval, which is every 90 minutes, by default. This refresh interval is configurable by a Group Policy administrator.

In contrast to Group Policy settings, Group Policy does not strictly enforce preferences. Group Policy does not store preferences in the Policy branches of the registry. Instead, it writes preferences to the same locations in the registry that the application or operating system feature uses to store the setting. The implication of this is twofold. First, Group Policy preferences support applications and operating system features that aren’t Group Policy-aware. Second, Group Policy preferences do not cause the application or operating system feature to disable the user interface for the settings they configure. The result is that after deploying preferences using Group Policy, users can still change those settings. Additionally, Group Policy refreshes preferences using the same interval as Group Policy settings by default. However, administrators can prevent Group Policy from refreshing individual preferences by choosing to apply them only once. This configures the preference one time and allows the user to change it permanently.

Group Policy filtering is substantially different from Group Policy preference item-level targeting. GPOs are filtered using WMI filters, and those filters determine whether Group Policy applies to the entire GPO. Individual policy settings within a GPO can’t be filtered. Of course, GPOs can be created based upon filtering requirements to work around this limitation, but that might lead to a large set of GPOs to manage. On the other hand, Group Policy preferences support item-level targeting—individual preference items can be targeted within a GPO. For example, a single GPO can contain two preference items, both of which configure power policies. The first preference item might target desktop PCs and the second mobile PCs. Additionally, while Group Policy filtering requires administrators to write sometimes complex WMI queries, item-level targeting provides a friendly user interface.

### Group Policy Preference Items

The following table provides an overview of the key functionality of each Group Policy preference extension:

Table 13

|  |  |
| --- | --- |
| **Windows Settings** | |
| **Map** **Drives** | Provides the ability to create, replace, update, and delete network drive mappings without logon scripts.  Multiple Drive Maps preference items can be deployed within a single GPO. Drive Maps preference items can target specific departments, locations, etc. |
| **Environment** | Enables the management of user and system environment variables.  Provides a way to configure variables for difference scenarios using a single GPO.  A location of a file repository can be defined using the Environment preference extension. That variable can then be used in other preference items rather than hard-coding the path. This results in a single GPO to update when the path changes, rather than having to find the path in other locations. |
| **Files** | Provides the ability to create, replace, update, and delete files on destination computers.  Supports wildcards in files paths, making it easy to copy groups of files using a single GPO.  A common scenario for using the Files preference extension is to copy configuration files to users’ profile folders. For example, this would allow the IT staff to copy custom dictionary or application files to the AppData folder within each user profile. |
| **Folders** | Allows the user to create, replace, update, delete, and even clean up folders on targeted computers.  Supports environmental variables, but does not support wildcards in folder paths.  The folders preference extension can be used to regularly clean up temporary folders. For example, this extension can be used to remove temporary folders that some applications create in the root of the system drive or to clean up the Windows temporary folder on a regular basis. |
| **Ini Files** | Provides the ability to create, update, replace, and delete individual properties from .ini files. |
| **Network Shares** | Supports managing network shares on multiple, targeted computers.  Allows the management of Access-based Enumeration (ABE), which prevents users from seeing subfolders for which they lack access permission, and to configure user limits. |
| **Registry** | Provides a flexible and easy-to-use way to create, replace, update, and delete registry settings on multiple computers.  Using the Registry preference extension is a great way to deploy settings without having to write scripts. For example, it can be used to deploy settings for a third-party application or an application that isn’t Group Policy-aware. |
| **Shortcuts** | Provides the ability to create, replace, update, and delete three types of shortcuts on multiple targeted users and computers:   * File System Object**—**Traditional shortcuts that link to programs and documents * URL—Shortcuts to Web pages * Shell Object—Objects that appear in the shell namespace, including Control Panel, Recycle Bin, etc.   The Shortcuts preference extension supports creating shortcuts in numerous locations, including the desktop, **Start** menu, Favorites folder and Quick Launch toolbar. |
| **Control Panel Settings** | |
| **Data Sources** | Provides a way to create, replace, update, and delete data sources for users and computers.  Allows user data sources to roam with users from computer to computer, further simplifying deployment.  Using the Data Sources extension reduces the complexity and cost of managing business applications which require data sources to be configured. |
| **Devices** | Provides a targeted method for disabling specific device classes for users or computers  Using the Devices extension, for example, provides the ability to disable the USB ports, floppy disk drives, and other removable media for users who work with sensitive information, such as customer records or intellectual property.  The Devices extension does not prevent users from installing devices. Rather, it enables or disables devices after they are present on the computer. |
| **Folder Options** | Supports two types of items:   * Folder Options—Configure Windows Explorer folder options for Windows XP or Windows Vista. * Open With—Configure associations between file extensions and file types. Two scenarios are common. First, file associations can be broken to prevent programs from running accidentally or maliciously (many e-mail viruses rely on file associations to run). Second, file extensions can be associated with different programs. |
| **Internet Settings** | Allows the configuration of Internet Explorer options for Microsoft Internet Explorer 5, Internet Explorer 6, and Internet Explorer 7.  Most of the settings that are available in the Internet Options control panel can be configured.  Many of these settings are available as Group Policy settings that are strictly enforced. The Internet Settings preference extension can be used to create a default Internet Explorer configuration that users can later change. |
| **Local Users and Groups** | Supports configuring local user accounts and groups for multiple, targeted computers. It supports these preference types:   * Local User—Allows the user to create, update, replace, or delete users account from local computers. For example, it can be used to change the password for or disable the local Administrator account. * Local Group—Provides the ability to create, update, replace, or delete groups from the local computer. For example, it can be used to add or remove a logged-on user to or from the group. |
| **Network Options** | Enables the configuration of the following types of network connections:   * VPN Connections—Configure Virtual Private Network (VPN) connections, including their options, security settings, and connection type. * DUN Connections—Configure basic Dial-Up |
| **Power Options** | The Power Options preference item can be used to configure power options and power schemes for computers running Windows XP. This enables the creation of a default configuration that users can later change as needed. |
| **Printers** | Configuring printer connections is a common task that administrators typically perform by writing logon scripts. The Printers preference extension provides the ability to easily create, update, replace, or delete shared printers, TCP/IP printers, and local printers to multiple, targeted users or computers.  Preference targeting can be used to deploy printer connections based on location, department, computer type, and so on. |
| **Regional Options** | Allows the configuration of the user locale, including number, currency, time, and date formats. |
| **Scheduled Tasks** | Provides a centralized mechanism for scheduling tasks for targeted users and computers. (The user interface for Scheduled Tasks preference items matches Scheduled Tasks in Windows.)  This preference extension makes it very easy to manage scheduled tasks using Windows Vista’s powerful new Task Scheduler. |
| **Services** | Enables the configuration of services in the following ways:   * Startup—Optionally change the startup type to Automatic, Manual, or Disabled. * Service action—Optionally start, stop, or restart a service. * Log on as—Configure the account that the service uses. * Recovery—Configure the service’s recovery options. |
| **Start Menu** | Provides the ability to configure **Start** menu options for users.  Supports both Windows XP and Windows Vista Start Menu preference items.  For instance, it can be used to configure the **Start** menu for mobile PCs so that it always displays the **Connect To** menu, or to easily configure the **Start** menu to reflect how the organization’s employees use their computers. |

### Group Policy Preference Features

Most Group Policy preference extensions support the following actions for each preference item:

* Create—Create a new item on the targeted computer.
* Delete—Remove an existing item from the targeted computer.
* Replace—Delete and recreate an item on the targeted computer. The result is that Group Policy preferences replace all existing settings and files associated with the preference item.
* Update—Modify an existing item on the targeted computer.

### Targeting Control

Targeting is a feature that makes preferences a particularly powerful way to deploy configurations.

GPOs can be filtered by using WMI filters; however, filters affect the entire GPO. To filter individual policy settings in a GPO, the work-around is usually to create separate GPOs for individual settings, and then to filter each GPO. In many organizations, this leads to hundreds, if not thousands, of GPOs that become unwieldy to maintain and have a significant impact on performance.

Group Policy preferences, however, support item-level targeting. Item-level targeting determines the users and computers to which Group Policy applies individual preference items within a GPO. For example, different preferences items can be targeted within a single GPO at computers in different locations.

Group Policy preference items provide the muscle to configure users and computers, but targeting items provides the logic needed to choose a limited selection of users and computers. Here are some real-world examples of how administrators can use Group Policy targeting items:

* Mobile computers—An organization may want to configure VPN connections, but may want to apply those VPN connections only to mobile PCs. The preference item can be limited to only mobile PCs by using the Portable Computer targeting item.
* Performance-based configuration—It might be required to configure certain settings based on the performance characteristics of each computer. Faster computers with plenty of free disk space may receive one preference item, while slower computers or those with low amounts of free disk space receive another. The CPU Speed and Disk Space targeting item may be used to target each preference item as required.
* Operating system version—With Windows Vista some settings are stored in a different location that with Windows XP. Two preference items can be created, one for each operating system. Each filter preference item can then be targeted using the Operating System targeting item.
* Software prerequisites—An application’s settings may need to be configured, but the administrators may first want to ensure that the application is actually installed on the computer before attempting to configure it. A combination of the File Match and Registry Match targeting items can be checked for a specific version of a binary file or an entry in the Uninstall registry key can provide a robust way to verify that the application is installed.

### Deploying Group Policy Preferences

Group Policy preferences do not require the installation of any services on servers. Windows Server 2008 includes Group Policy preferences by default as part of the Group Policy Management Console (GPMC). Administrators will also be able to configure and deploy Group Policy preferences in a Windows Server 2003 environment by installing the RSAT on a computer running Windows Vista with SP1. Both RSAT and Windows Vista SP1 will be available in the first quarter of 2008.

Although no services need to be installed to create GPOs that contain Group Policy preferences, the Group Policy preferences client-side extension (CSE) must be deployed to any client computer to which preferences will be deployed. The CSE will be available as a separate download from Microsoft. It supports the following Windows versions:

* Windows XP with SP2
* Windows Vista
* Windows Server 2003 with SP1
* Windows Server 2008 already includes the CSE

### Benefits of Group Policy Preferences

The following list summarizes the benefits of using Group Policy preferences:

* Improving IT Productivity—Group Policy preferences extends the Group Policy feature set with more than 20 new extensions, enabling the IT staff to get more done with tools that are already familiar. It also enables the configuration and deployment of settings at a central source, rather than repackaging and redeploying the settings when updating configurations. Administrators simply edit the GPO that contains the preference items that they want to update. Preferences provide a central location from which user and computer configurations can be managed.
* Reducing Need for Logon Scripts—Although Group Policy preferences might not eliminate the need for logon scripts, it significantly reduces their need. The most common tasks performed by logon scripts are installing printers, mapping network drives, configuring registry settings, and copying files and folders.
* Limiting Configuration Errors—Configuration errors during and after deployment are often a significant source of support calls that lead to higher deployment costs. Group Policy preferences help to lower these costs. First, preferences allow the configuration of items with a higher level of precision than other tools. Second, items can be configured without knowing their details. Instead, Group Policy preferences collects preference items using clear, familiar, easy-to-use dialog boxes that prevent the user from needing to know how Windows stores the value in the registry. Administrators can configure a **Start** menu setting by selecting an option in a preference item instead of having to know what value to store in the registry and where to store it. Group Policy preferences all but eliminate the need to use default user profiles to deploy settings. With a default user profile, far more is often deployed than is needed; and this can lead to unreliable configurations.
* Enhancing End-User Satisfaction—More consistent, reliable configurations make users happy by maintaining or even increasing their productivity. Additionally, using Group Policy preferences to configure users and computers can make using Standard user accounts more palatable to users. Group Policy preferences use the local System account by default, enabling it to configure settings that users can’t configure. By configuring these settings on behalf of users, administrators can often avoid the issue altogether.
* Minimizing Image Maintenance—Using Group Policy preferences with a thin-image strategy can significantly reduce the time and cost of maintaining disk images. Instead of updating images to reflect configuration changes, a generic image can be deployed and then administrators can update Group Policy preferences. This approach reduces engineering and testing time—and costs—significantly.
* Reducing Overall Image Count—Group Policy preferences, in combination with a thin-image strategy, helps reduce the number of disk images that must be developed and maintained. Building thick images often creates unique images for different groups of users within the organization. With Group Policy preferences, the IT department can instead build and deploy a generic image for each group and then configure users and computers uniquely by targeting preference items.

## Windows Remote Management (WS-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. Unlike DCOM-based remote access, Windows Remote Management and WS-Management uses standard, fixed ports. This provides an elevated level of security since SW-Management uses a standard fixed port, as opposed to the dynamic port model used by DCOM-based access.

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. For example, information can be obtained from local and remote computers about objects such as disks, network adapters, services, or processes. If the computer runs a Windows operating system version that includes Windows Remote Management, the management data is supplied by Windows Management Instrumentation (WMI). Hardware and system data can also be obtained from WS-Management protocol implementations running on non-Windows operating systems. Data returned to WS-Management protocol are formatted in XML rather than in objects.

### Windows Remote Shell

IT Professionals can use the new Windows Remote Shell (WinRS) tool to remotely manage servers or to obtain management data through Windows Remote Management and Windows Management Instrumentation (WMI) objects on remote servers. Windows Remote Shell allows remote execution of scripts on Windows Vista and Windows Server 2008 computers. WinRS leverages the Microsoft implementation of the DMTF-standard WS-Management remote access protocol.

## 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

The server core installation of Windows Server 2008 supports the following optional features:

* Failover Clustering
* WINS
* Network Load Balancing
* Subsystem for UNIX-based applications
* Backup
* Multipath IO
* Removable Storage Management
* BitLocker Drive Encryption
* Simple Network Management Protocol (SNMP)
* Distributed File System Replication
* Simple Network Time Protocol (SNTP)

To accomplish this, the Server Core installation option installs only the executable files and supporting dynamic link libraries (DLLs) required by the roles selected for the server. For example, the Windows Explorer user interface (or "shell") is not installed as part of Server Core. Instead, when using a Server Core–based server, the default user interface is the command prompt.

Server Core offers the following benefits to organizations:

* Reduced software maintenance—Because Server Core installs only what is required to support the installed 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. With a minimal Server Core installation, there are fewer installed components that will need to be updated or patched, and the number of required restarts will be reduced.
* 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 Server Core installation installs the minimal files needed to provide the required functionality, so less disk space will be used on the server.

Server Core is designed for use in organizations that either have many servers, some of which need only to perform dedicated tasks, or in environments where high security is a requirement.

Because no graphical user interface is available for many Windows Server operations, using the Server Core installation option requires administrators to manage the Server Core installation with Microsoft Management Console (MMC) snap-ins from another computer running Windows Server 2008, by selecting the Server Core computer as a remote computer to manage, or to be experienced in using a command prompt or scripting techniques for local administration of the server.

### Not an Application Platform

Server Core is not an application platform, and users cannot run or develop server applications on a Server Core installation. A Server Core installation can only be used to run the supported server roles and management tools.

Server Core does support management tools and agents, which can be divided into two categories:

* Remote Management tools—these tools do not require any changes, as long as they use one of the protocols supported by a Server Core installation to communicate with the remote management workstation, such as RPC.
* Local Management tools and agents—these tools might require changes to work with a Server Core installation, since they cannot have any shell or user interface dependencies, nor use managed code.

The Windows Server 2008 Software Development Kit (SDK) includes a list of APIs that are supported on a Server Core installation.

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.

## Enterprise Class Print Management

The larger the organization, the larger the number of printers within the network, 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 error conditions, and can also send notifications in e-mail, 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.

The administrator on the local print server can add and remove printers. Print Management can automatically detect all printers located on the same subnet as the print server, install the appropriate printer drivers, set up the queues, and share the printers. Unless a printer driver cannot be found, no intervention is needed.

Print Management provides centralized administration of all of the printers in the organization from any computer running Windows Server 2003 R2, Windows Vista, or Windows Server 2008 operating systems. Print Management is also available for Windows XP clients, both x86 and x64.

### Managing Printers

Print Management can be used to manage all of the printers in the entire enterprise, including printers in branch offices. The same interface is used to control how printers are shared, update drivers, and control print queues, regardless of the actually physical location of the specific printer. It is unnecessary to navigate to the individual folders for each printer on each print server. By using Print Management in conjunction with the Configure Your Server Wizard and Terminal Services, administrators can automatically search for and install network printers on a local print server in branch offices. This is helpful when branch office personnel are not trained in administrative duties.

### Listing and Removing Printers in Active Directory

Listing printers in the Active Directory makes it easier for administrators to locate and install printers. After printers have been installed on a print server, administrators can use Print Management to list them in Active Directory. In fact, administrators can list more than one printer simultaneously. Administrators may want to set up a filter to show all of the printers to list or remove, so that they can easily select all of the printers at the same time.

### Deploying Printers by Using Group Policy

Print Management can be used with Group Policy to automatically add printer connections to a client computer's Printers and Faxes folder. A printer connection setting can be automatically added to an existing Group Policy object (GPO) in Active Directory. When Group Policy processing runs on client computers, the printer connection settings are applied to the users or computers associated with the GPO. Printers deployed by using this method appear in the Deployed Printers object of Print Management tree when the print server they are connected to is being monitored.

This method of installing a printer is useful in laboratory, classroom, or branch office settings where every computer in the room or office needs access to the same printer. It is also useful in large organizations, where computers and printers are often separated by function, workgroup, or department. A printer connection that has been installed by using a per-user connection is available to the user, no matter what computer the user logs on to. A printer connection that has been installed by using a per-computer connection appears in the Printers and Faxes folder and is available to any user of that computer.

### Troubleshooting Printers

Print Management has several features that may help identify and resolve printer problems—even in remote locations. Setting pre-defined filters lets administrators easily find all printers that are not in Ready status or that have print jobs backed up queue. Many devices, regardless of manufacturer, provide rich status information, which is readily available to Print Management. By closely monitoring the printers within the organization, administrators may even be able to resolve problems before they happen, such as identifying when paper or toner is low. E-mail message notifications can be set up to alert administrators when a printer needs attention. This is especially useful when the organization has printers at multiple locations with different people responsible for managing them. By using an automated system to notify the IT staff when a printer or print server is unavailable, the problem may be resolved sooner reducing the impact of printer and print server problems.

### Key Benefits

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.

## 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.

### Enhancements to Windows Deployment Services

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. Microsoft Deployment unifies the tools and processes required for desktop and server deployment into a common deployment console and collection of guidance. The fourth generation deployment accelerator adds integration with recently released Microsoft deployment technologies to create a single path for image creation and automated installation. Microsoft Deployment’s tools and end-to-end guidance reduce deployment time, standardize desktop and server images, limit service disruptions, reduce post-deployment help desk costs, and improve security and ongoing configuration management. More information can be found at: <http://www.microsoft.com/downloads/details.aspx?familyid=3bd8561f-77ac-4400-a0c1-fe871c461a89&displaylang=en&tm>

## New Active Directory Domain Services Installation Wizard

To simplify the installation, a new installation wizard is included in Windows Server 2008. In the new wizard, for example, all error-checking for local network settings, such as TCP/IP and Domain Name System (DNS) client settings are grouped together. Functionality that is relevant only to the creation of a new domain, such as NetBIOS name and Anonymous Access permissions, are located near the selection of a new domain.

The Active Directory Domain Services Installation Wizard contains a new option on the Welcome page of the wizard to enable Advanced mode, as an alternative to running dcpromo with the "/adv" switch (for example, dcpromo /adv). Advanced mode exposes additional options that enable more advanced configurations and provide experienced users with more control over the operation, including:

* Creating a new domain tree
* Leveraging backup media from an existing domain controller in the same domain to reduce network traffic associated with initial replication
* Selecting the source domain controller for the installation
* Defining the password replication policy for a Read Only Domain Controller (RODC)

In addition to these changes, the Active Directory Domain Services Installation Wizard has new dialog-box pages, which are listed in the following table:

Table 14: AD DS Installation Wizard Options

|  |  |
| --- | --- |
| **New wizard page** | **Description** |
| Additional options | Specifies that during the domain controller installation, the domain controller will also be configured to be a DNS server, global catalog server, or RODC. |
| Site selection | Specifies the site in which the domain controller should be installed. |
| Set functional levels | Sets the domain and forest functional level during the installation of a new domain or forest. |
| Password Replication Policy | Specifies which account passwords to allow or deny from being cached on an RODC. This page appears only if the UseAdvanced mode installation check box is selected. |
| DNS delegation creation | Provides a default option to create a DNS delegation based on the type of domain controller installation (as specified on the Choose a Deployment Configuration page) and the DNS environment. |

Other improvements reduce the chances of errors occurring during AD DS installation. For example, when installing an additional domain controller, the user can select the domain name from a domain tree view rather than having to type it.

New options for running unattended installation of AD DS are available in Windows Server 2008. Unlike unattended installation in the Windows Server 2003 operating system, unattended installation in Windows Server 2008 never requires a response to any user interface prompt, such as a prompt to restart the domain controller. This is necessary to install AD DS on a Server Core installation of Windows Server 2008, a new installation option for Windows Server 2008 that does not provide user interface options such as the interactive Active Directory Domain Services Installation Wizard.

## Restartable Active Directory Domain Services (AD DS)

Administrators can stop and restart Active Directory Domain Services (AD DS) in Windows Server 2008 by using Microsoft Management Console (MMC) snap-ins or the command line. Restartable AD DS reduces the time that is required to perform certain operations such as applying updates to the server. Administrators can also stop AD DS to perform tasks, such as offline defragmentation of the Active Directory database, without restarting the domain controller. Other services that are running on the server and that do not depend on AD DS to function, such as Dynamic Host Configuration Protocol (DHCP), remain available to satisfy client requests while AD DS is stopped.

Although stopping AD DS is similar to logging on in Directory Services Restore Mode, the restartable AD DS provides a unique state for a domain controller running Windows Server 2008. This state is known as AD DS Stopped. The three possible states for a domain controller running Windows Server 2008 are:

* AD DS Started—In this state, AD DS is started. For clients and other services running on the server, a Windows Server 2008 domain controller running in this state is the same as a domain controller running Windows 2000 Server or Windows Server 2003.
* AD DS Stopped—In this state, AD DS is stopped. Although this mode is unique, the server has some characteristics of both a domain controller in Directory Services Restore Mode and a domain-joined member server.
* As with Directory Services Restore Mode, the Active Directory database (Ntds.dit) is offline. Also, the Directory Services Restore Mode password can be used to log on locally if another domain controller cannot be contacted for logon.
* As with a member server, the server is joined to the domain. Users can log on interactively or over the network by using another domain controller for domain logon. However, a domain controller should not remain in this state for an extended period because in this state, it cannot service logon requests or replicate with other domain controllers. When the client renews its association with the DC, if the original DC is back up and running, it will revert back to that association.
* Directory Services Restore Mode—This mode (or state) is unchanged from Windows Server 2003.

The following flowchart shows how a domain controller running Windows Server 2008 can transition between these three possible states.

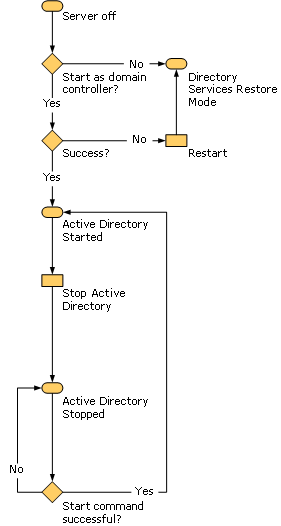


Figure 11: Three states of domain controller running Windows Server 2008

With new installation options such as RODC, helpful wizards and improved management interfaces and tools, Active Directory Domain Services services in Windows Server 2008 simplifies the remote deployment and on-going management of domain controllers and domain services at remote locations.

## Active Directory Domain Services Snapshot Viewer

Windows Server 2008 includes an enhanced ntdsutil command that can be used to create AD DS snapshots. These snapshots capture the complete state of Active Directory at the time they are made. Existing AD DS snapshots can be mounted as a parallel read-only instance of Active Directory without starting the domain controller in Directory Services Restore Mode. Mounting an AD DS snapshot can be used to recover deleted or modified AD DS objects.

The Snapshot Viewer in Windows Server 2008 helps administrators identify objects that have been accidentally deleted by exposing information about the objects in snapshots of the AD DS that are taken over time. By comparing the various states of the objects as they appear in different snapshots, administrators can better decide which AD DS snapshot to use to restore the deleted objects.

## Summary

Tools, technologies, and installation options are available in Windows Server 2008 that improve the management experience of single and multiple servers across an enterprise and simplify the deployment of Windows operating systems.

Server Manager is an integrated Microsoft Management Console that offers IT Professionals an integrated experience for adding, remove, and configuring server roles, roles services, and features. It also acts as a portal for ongoing server management, monitoring and operations, by exposing key management tasks based on server role, and providing access to advanced administration tools.

Management of multiple servers can be automated using Window PowerShell, which consists of a new command-line shell and scripting language designed specifically to automate administration tasks for server roles, such as IIS and Active Directory.

With the Server Core installation option in Windows Server 2008, administrators can reduce the ongoing maintenance requirements for servers, and simplify their management by installing only the required functionality on the server.

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

# Chapter 8: High Availability

## Introduction

Availability refers to a level of service provided by applications, services, or systems. A highly available system provides an acceptable level of service with minimal downtime. Excessive, unanticipated downtime can have a significant negative impact on an organization. Loss of critical systems, services or applications can reduce employee productivity, sales, and confidence from partners and customers. Ensuring that critical applications and services are always highly available is a key priority for IT departments, and High Availability is a central theme in many of the enhancements made in Windows Server 2008.

This chapter will introduce some of the key features in Windows Server 2008 that help ensure high availability while simplifying management:

* Failover Clustering
  + Ensures that a hardware failure will not impact the availability of mission-critical applications and services
  + Provides new features that make failover clusters easier to implement, configure and maintain making failover clusters a smart business choice
* Server Manager Console
  + Reduces complexity, providing the user with a simple interface to create, manage and use clustered servers
  + Reduces support costs and implementation times due to reduced number of deployment and configuration issues
  + Enhances functionality that allows implementation in geographically dispersed environments, allowing the technology to adapt to the customers’ environment
* Network Load Balancing
  + Network load balancing distributes the load for networked client/server applications across multiple cluster servers
  + NLB in Windows Server 2008 includes improvements to networking, security and management which increase availability and reliability
* Improved Backup
  + Improves backup speed
  + Simplifies restoration
  + Improves scheduling

## Failover Clustering

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. 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 need to 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.

### New Functionality in failover clustering

#### New validation wizard

The complete configuration—servers, network, and storage—must be carefully configured to fully realize the benefits of high availability. The setup and configuration of Failover Clusters has been 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—analyzes whether the storage is correctly configured so that all cluster nodes have access to all shared disks and meet specified requirements

### Enhanced scalability for large volumes

Windows Server 2008 includes support for global unique identifier, or GUID Partition Table (GPT) disks in cluster storage. GPT disks can have partitions larger that 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.

### Improvements in failover clusters

Failover clusters in Windows Server 2008 incorporate the following improvements to cluster deployment, management, and operation:

* Improved cluster setup and migration—The Cluster Setup wizard is simplified so that the user can set up a cluster in one step. Cluster setup is also now fully scriptable so that deployment can be automated. Migration of an existing cluster is simplified. Resource group settings can be captured from a cluster running Windows Server 2003 and applied to a cluster running Windows Server 2008.
* Simplified management interfaces—With wizards and interface improvements, management tasks are simplified and administrators can focus on managing their applications, not their cluster.
* Improvements to stability and security, resulting in increased availability—The way the cluster communicates with storage has been improved so that the quorum resource is no longer a single point of failure.
* Improvements to networking and security—Network performance and security are improved through the integration of IPv6, the use of DNS without legacy NetBIOS dependencies, as well as other networking improvements that help organizations achieve better reliability and a more secure deployment.

#### Server Manager Console

To simplify the management of clusters, the management interfaces have been 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. With failover clusters in Windows Server 2008, the following management and operation tasks are simplified:

* Improved interface—The user interface is now task-based, supported by wizards that guide administrators through what were previously complex operations. Now, setting up cluster roles, such as a printer server role, only takes a few easy steps. The new cluster administration tool provides a complete view of the clustered roles, providing configuration options as intuitive task-based menu choices.
* Quickly add clustered resources to the configuration—Tasks, such as making a shared folder highly available are also easier to perform with the improved cluster management interface.
* Troubleshoot a cluster—Instead of working with the cluster log, administrators can use Event Tracing for Windows to easily gather, manage, and report information about the sequence of events occurring on the cluster.
* Use the Volume Shadow Copy Service to capture backups—Full integration with the Volume Shadow Copy Service makes it easier to back up and restore the cluster configuration.
* Control the way shared folders in a cluster are viewed—The system scopes the view of shared storage, and accordingly, shared folders. This makes it easy to understand which shared folders are clusters and capable of being failed over to another node, and which shared folders are local to a single node and cannot failover.

Windows Server 2008 also supports command line and Windows Management Instrumentation (WMI) options for failover clusters.

### Improved Stability

With failover clusters in Windows Server 2008, many improvements to the cluster infrastructure help maximize user services. One of the more significant changes is how the system maintains the “quorum.” Quorum is the cluster’s configuration database that determines which nodes are active and which nodes are in standby. It is used to ensure that, if communications between nodes are interrupted, only one node continues to offer the applications and services. If there is a loss of communication between cluster nodes, a challenge response protocol is initiated to prevent a split-brain scenario. When there is a loss of communication, the owner of the cluster resource becomes the only owner of the cluster and all of the resources, preventing the split brain. The owner then makes the resources available for clients. When the node that owns the quorum disk functions incorrectly, the surviving nodes arbitrate to take ownership of the device.

With the improvements in failover clusters, administrators can configure the cluster with either of the two cluster models that were available in previous versions of Windows:

* The quorum disk model: a single disk is the “voter” that determines which parts of a fragmented cluster are allowed to continue
* The majority node set model: the cluster operates only if the majority of the nodes are healthy and communicating

With Windows Server 2008, a new “hybrid” of the two models is now the default configuration. This offers the advantages of both models. For example, with a two-node cluster, the cluster continues running even if the quorum disk has completely failed. Administrators do not have to deal with the complexities of configuring the quorum; that is all done automatically during cluster setup. With this new hybrid model each node has a replica of the quorum resource, so the failure of the quorum disk no longer results in the failure of the cluster.

### Storage integration

Enhancements in storage integration in Windows Server 2008 failover clusters provide better functionality and reliability than in previous releases of server clusters. Key improvements include:

* Dynamic addition of disk resources—Resource dependencies can be modified while resources are online, which means administrators can make an additional disk available without interrupting the applications that will use it.
* Improved performance and stability with data storage—Windows Server 2008 contains enhanced mechanisms to use Persistent Reservations and a new algorithm for managing shared disks. It no longer uses SCSI Bus Resets which can be disruptive on a SAN. With failover clustering in Windows Server 2008, 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.

### Networking and security

With failover clusters in Windows Server 2008, network performance and security are improved, compared with previous releases. Improvements allow the user to:

* Use IPv6, which is fully integrated into failover clusters—Failover clusters fully support IPv6 for both node-to-node and node-to-client communication.
* Use Domain Name System (DNS) without legacy NetBIOS dependencies—This simplifies the transport of Server Message Block (SMB) traffic, and means users do not have Windows Internet Name Service (WINS) and NetBIOS name-resolution broadcasts.
* Achieve better reliability through other improvements to networking—Administrators can create associations between a network name resource and multiple associated IP addresses so that the network name will be available if any of the IP addresses are available. In addition, when nodes transmit and receive "heartbeats" to confirm that each node is still available, they use the more reliable Transmission Control Protocol (TCP) rather than the less reliable User Datagram Protocol (UDP).
* Provide enhanced security. Security improvements in failover clusters include:
  + A new security model—Windows Server 2008 contains an improved Security Model in which the Cluster Service now runs in the context of the LocalSystem built-in account. This increases security and enhances account password management.
  + Auditing—Administrators can use auditing to capture information about who accessed a cluster and when it was accessed.
  + Encryption—Windows Server 2008 allows administrators set inter-node communication to be encrypted.
* Support nodes on different IP subnets—Nodes in the cluster no longer need to be on the same IP subnet providing greater flexibility. This is particularly useful when clusters are being stretched across geographical distance to provide site resiliency.

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, 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 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 provides scalability by allowing additional servers to be added as load increases. NLB provides reliability by allowing users to easily replace a malfunctioning server. 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 (IIS), can be scaled out by adding additional servers as the work load increases.

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, 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.
* Improved denial of server (DOS) attack and timer starvation protection—Using a callback interface, NLB can detect and notify applications when an attack is underway or when a node is under excessive load. Microsoft ISA Server 2006 uses this functionality in scenarios where the cluster node is overloaded or is being attacked.
* Support for multiple dedicated IP addresses per node—NLB fully supports defining more than one dedicated IP address for each node (previously only one dedicated IP address for each node was supported). This allows multiple applications to be hosted on the same NLB cluster in scenarios where separate applications require their own dedicated IP address. The Microsoft NLB\_NodeSetting class supports multiple dedicated IP addresses by specifying them in DedicatedIPAddresses and DedicatedNetMasks. This functionality is used by ISA Server 2006 to manage each NLB node for scenarios where the clients consist of both IPv4 and IPv6 traffic.

These network load balancing 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 key component of Windows Server 2008 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. 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.

### New Backup functionality

Key improvements in Backup include:

* + New, faster backup technology—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.
  + Simplified backup—After the first full backup is created, Backup automatically runs incremental backups, saving only the data that has changed since the last backup occurred. Unlike previous versions of Backup, administrators no longer have to worry about manually scheduling full and incremental backups.
  + Simplified restoration—Items can now be restored by choosing a backup and then selecting items to restore from that backup. Individual files or entire folders can be recovered. Previously, it was necessary to manually restore from multiple backups if the item was stored on an incremental backup. Now, the user can simply choose the backup date for the items they wish to restore.
  + Simplified recovery of the operating system—Backup works with the new Windows Recovery tools to make it easier to recover the operating system. Users can recover to the same server, or, if the hardware fails, he or she can recover to a new server that has no operating system.
  + Support for DVD media—Users can manually back up volumes directly to DVD. Backup also retains support for backing up manually to shared folders and hard disks. Scheduled backups are stored on hard disks.
  + Improved Scheduling—Backup now includes a wizard to guide the IT staff through the process of creating daily backups. System volumes are automatically included in all scheduled backups.

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 up data recovery.

## Windows Reliability and Performance Monitor

Windows Server 2008 includes the Windows Reliability and Performance Monitor, which provides IT Professionals with tools to easily monitor and assess system performance and reliability. (Note: In some pre-release versions of Windows Sever 2008, this feature was called “Windows Performance Diagnostic Console.”) Windows Reliability and Performance Monitor is an MMC snap-in that combines the functionality of several previous stand-alone tools, including Performance Logs and Alerts, Server Performance Advisor, and the System Monitor. It provides an easy-to-use graphic interface for customizing performance data collection and Event Trace Sessions. It also includes Reliability Monitor, another MMC snap-in that tracks changes to the system and compares them to changes in system stability, providing a graphical view of their relationship.

Windows Reliability and Performance Monitor is a tool designed to provide IT Professionals and network administrators with the performance information needed to effectively manage their networks. To view real-time status in Resource View, the console must run as a member of the Administrators group. To create Data Collector Sets, configure logs, or view reports, the console must run as a member of the Administrators group or the Performance Log Users Group.

### New monitoring features

The following are key features of the new Windows Reliability and Performance Monitor included in Windows Server 2008:

* Data Collector Sets
* Wizards and templates for creating logs
* Resource View
* Reliability Monitor
* Unified property configuration for all data collection, including scheduling
* User-friendly diagnosis reports

#### Data Collector Sets

The Data Collector Set is an important new feature in the Windows Reliability and Performance Monitor that groups data collectors into reusable elements for use with different performance monitoring scenarios. For an administrator managing multiple servers, this can save time, because a Data Collector can be defined once, specifying what information needs to be monitored, and then used on multiple servers. When a group of data collectors are stored as a Data Collector Set, operations such as scheduling can be applied to the entire set through a single property change. A default Data Collector Set template is also included in the Windows Reliability and Performance Monitor to allow system administrators to immediately begin collecting performance data specific to a Server Role or monitoring scenario.

#### Wizards and templates for creating logs

Adding counters to log files and scheduling their start, stop, and duration, can now be performed through a simplified wizard interface. Saving this configuration as a template allows system administrators to collect the same log on subsequent computers without going through the configuration steps on every computer. Performance Logs and Alerts features are now incorporated into the Windows Reliability and Performance Monitor for use with any Data Collector Set.

#### Resource View

The new Resource View screen is now the home page of the Windows Reliability and Performance Monitor. This view provides a real-time graphical overview of CPU, disk, network, and memory usage. By expanding each of these monitored elements, system administrators can identify which processes are using which resources. In previous versions of Windows, this real-time process-specific data was only available in limited form within the Task Manager.

#### Reliability Monitor

The Reliability Monitor calculates a System Stability Index that reflects whether unexpected problems reduced the reliability of the system. A graph of the Stability Index over time quickly identifies dates when problems began to occur. The System Stability Report provides details to help troubleshoot the root cause of the problem. By viewing changes to the system, such as installation or removal applications, updates to the operating system, modification of drivers, side by side with failures—application failures, hardware failures, ore operating system stops—a strategy for addressing the issues can be developed quickly, saving time and resources.

#### Unified property configuration for data collection

Whether creating a Data Collector Set for one-time use or to log activity on an ongoing basis, the interface for creation, modification, and scheduling is the same. If a Data Collector Set proves to be useful for future performance monitoring, it does not need to be re-created. It can be reconfigured or saved as a template. This simplified process will save administration time while providing more effective monitoring of performance information.

#### User-friendly diagnosis reports

Users familiar with the Server Performance Advisor in Windows Server 2003 can now find the same kinds of diagnostic reports in the Windows Reliability and Performance Monitor in Windows Server 2008. The time required to generate reports is also improved. Reports can be created from data collected by using any Data Collector Set. This allows system administrators to easily duplicate reports and assess how changes to a server have affected performance or review the report's recommendations.

## Policy-based Quality of Service

Quality of Service (QoS) policies in Windows Server 2008 and Windows Vista allow network administrators to prioritize traffic between specified clients and servers, or between application servers. The prioritization settings can target specific application names, specific source and destination IP addresses, and specific source and destination TCP or UDP ports. QoS policy settings are configured as part of the user or computer configuration Group Policy settings in Active Directory.

To manage the use of bandwidth, administrators can configure a QoS policy with a throttle rate for outbound traffic. By using throttling, a QoS policy can limit the aggregate outbound network traffic to a specified rate. To specify prioritized delivery, traffic is marked with a Differentiated Services Code Point (DSCP) value. The routers or wireless access points in the network infrastructure can place DSCP-marked packets in different queues for differentiated delivery if the network components are QoS capable. Both DSCP marking and throttling can be used together to manage traffic effectively. Because the throttling and priority marking are taking place at the network layer, applications do not need to be modified.

For example, an administrator could configure QoS policy settings to ensure that traffic going to servers that host financial applications is prioritized for users in the Finance department, ensuring that group will get the fastest possible communications during peak usage.

## Summary

Failover clustering in Windows Server 2008 provides an easy-to-use solution for organizations needing to deliver critical applications and services. The new configuration features make it easier to design and deploy a high-availability failover cluster solution, and the new management interface reduces complexity and costs by providing a simple unified interface to manage failover clusters.

Network Load Balancing improves scalability and availability by distributing client traffic across multiple servers included in a cluster. Windows Server 2008 includes a variety of new features to simplify the administration of the cluster, and to improve an organization’s ability to effectively deliver mission-critical applications and services with a cluster solution. Improvements include support for IPv6 and NDIS 6.0, and enhanced functionality with ISA Server 2006.

The improved backup and recovery features in Windows Server 2008 allow administrators to efficiently and reliably protect not only critical data, but server operating systems and configurations as well. Wizards reduce management time and costs by providing easy-to-use tools for both backup and recovery.

The Quality of Service policy features in Windows Server 2008 enable network administrators to prioritize traffic between specified clients and servers, or between application servers, to ensure that the mission-critical applications and services get priority allocation of the available bandwidth resources.

# Chapter 9: 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, speeding up deployment and maintenance of IT systems, making consolidation and virtualization of servers and applications easier, and providing 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.

1. RADIUS is an Internet Engineering Task Force (IETF) standard. [↑](#footnote-ref-2)