

# Windows Server® 2008 Security Resource Kit

*Jesper M. Johansson and  
MVPs with the Microsoft  
Security Team*

To learn more about this book, visit Microsoft Learning at  
<http://www.microsoft.com/MSPress/books/11841.aspx>

9780735625044

**Microsoft®**  
Press

# Table of Contents

Acknowledgements .....xv

Introduction .....xvii

**Part I    Windows Security Fundamentals**

**1    Subjects, Users, and Other Actors .....3**

    The Subject/Object/Action-Tuple ..... 3

    Types of Security Principals..... 4

        Users..... 4

        Computers..... 7

        Groups ..... 7

        Abstract Concepts (Log-on Groups) ..... 10

        Services ..... 11

    Security Identifiers ..... 12

        SID Components..... 12

        SID Authorities ..... 13

        Service SIDs..... 14

        Well-Known SIDs ..... 15

    Summary ..... 16

    Additional Resources ..... 16

**2    Authenticators and Authentication Protocols..... 17**

    Something You Know, Something You Have ..... 17

        Something You Know ..... 18

        Something You Have ..... 18

        Something You Are ..... 18

    Understanding Authenticator Storage ..... 19

        LM Hash..... 21

        NT Hash ..... 23

 **What do you think of this book? We want to hear from you!**

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

[www.microsoft.com/learning/booksurvey/](http://www.microsoft.com/learning/booksurvey/)

Password Verifier .....	24
In Memory .....	25
Reversibly Encrypted .....	27
Authentication Protocols .....	29
Basic Authentication .....	29
Challenge-Response Protocols .....	30
Smart Card Authentication .....	37
Smart Cards and Passwords .....	38
Attacks on Passwords .....	38
Obtaining Passwords .....	38
Using the Captured Information .....	42
Protecting Your Passwords .....	44
Managing Passwords .....	46
Use Other Authenticators .....	46
Record Passwords, Safely .....	46
Stop Thinking About Words .....	47
Set Password Policies .....	47
Fine-Grained Password Policies .....	49
Summary .....	54
Additional Resources .....	54
<b>3 Objects: The Stuff You Want .....</b>	<b>55</b>
Access Control Terminology .....	55
Securable Objects .....	56
Security Descriptors .....	56
Access Control List .....	58
Access Control List Entry .....	59
Access Masks .....	61
Relationship Between Access Control Structures .....	66
Inheritance .....	66
Security Tokens .....	70
Access Check Process .....	72
Integrity Labels .....	74
Empty and NULL DACLs .....	75
Security Descriptor Definition Language .....	75
Tools to Manage Permissions .....	79
caccls and icaccls .....	79

SC .....	81
subinacl .....	81
Major Access Control Changes in Windows Server 2008.....	81
TrustedInstaller Permissions .....	81
Network Location SIDs .....	82
File System Name Space Changes.....	82
Power User Permissions Removed.....	82
OWNER_RIGHT and Owner Rights .....	82
User Rights and Privileges.....	83
RBAC/AZMAN.....	88
Summary .....	88
Additional Resources .....	89
<b>4     Understanding User Account Control (UAC).....</b>	<b>91</b>
What Is User Account Control? .....	92
How Token Filtering Works.....	92
Components of UAC .....	94
UAC Elevation User Experience .....	94
Application Information Service .....	98
File and Registry Virtualization .....	98
Manifests and Requested Execution Levels .....	100
Installer Detection Technology.....	101
User Interface Privilege Isolation.....	102
Secure Desktop Elevation Prompts .....	102
Using Remote Assistance .....	103
UAC Remote Administrative Restrictions .....	103
Mapping Network Drives When Running in Admin Approval Mode .....	104
Application Elevations Blocked at Logon.....	106
Configuring Pre-Windows Vista Applications for Compatibility with UAC.....	107
UAC Group Policy Settings .....	108
UAC Policy Settings Found Under Security Options.....	108
Related UAC policies .....	110
What's New in UAC in Windows Server 2008 and Windows Vista SP1 .....	111
New Group Policy Setting: UIAccess Applications to Prompt for Elevation without Using the Secure Desktop.....	112
UAC Prompt Reduction When Performing File Operations in Windows Explorer .....	112

	More Than 40 Additional UAC-Related Application Compatibility Shims .....	112
	UAC Best Practices .....	112
	Good Practice .....	112
	Better Practice .....	113
	Best Practice .....	113
	Summary .....	113
	Additional Resources .....	114
<b>5</b>	<b>Firewall and Network Access Protection .....</b>	<b>115</b>
	Windows Filtering Platform .....	116
	Windows Firewall with Advanced Security .....	118
	Improvements in the Windows Firewall .....	118
	Managing the Windows Firewall .....	122
	Routing and Remote Access Services .....	130
	Improvements in RRAS .....	131
	Internet Protocol Security .....	133
	IPsec Basics .....	133
	New Capabilities in Windows Server 2008 .....	136
	Network Access Protection .....	139
	Architecture .....	140
	NAP Implementation .....	143
	NAP Scenarios .....	146
	Summary .....	150
	Additional Resources .....	150
<b>6</b>	<b>Services .....</b>	<b>151</b>
	Introduction to Services .....	151
	What Is a Service? .....	152
	Service Logon Account .....	152
	Service Listener Ports .....	154
	Configuring Services .....	155
	Windows Server 2008 Services by Role .....	161
	Attacks on Services .....	161
	Blaster Worm .....	161
	Common Service Attack Vectors .....	163
	Service Hardening .....	165
	Least Privilege .....	165

Service SIDs . . . . .	170
Write Restricted SIDs . . . . .	172
Restricted Network Access . . . . .	174
Session 0 Isolation . . . . .	176
Mandatory Integrity Levels . . . . .	176
Data Execution Prevention . . . . .	176
Other New SCM Features . . . . .	177
Securing Services . . . . .	178
Inventory Services . . . . .	178
Minimize Running Services . . . . .	178
Apply a Least-Privilege Model to Remaining Services . . . . .	179
Keep Your Updates Up To Date . . . . .	179
Creating and Using Custom Service Accounts . . . . .	180
Use Windows Firewall and IPsec for Network Isolation . . . . .	181
Auditing Service Failures . . . . .	181
Develop and Use Secure Services . . . . .	182
Summary . . . . .	182
Additional Resources . . . . .	182
<b>7 Group Policy . . . . .</b>	<b>183</b>
What Is New in Windows Server 2008 . . . . .	183
Group Policy Basics . . . . .	184
The Local GPO . . . . .	184
Active Directory-Based GPOs . . . . .	185
Group Policy Processing . . . . .	190
What Is New in Group Policy . . . . .	194
Group Policy Service . . . . .	194
ADMX Templates and the Central Store . . . . .	194
Starter GPOs . . . . .	197
GPO Comments . . . . .	198
Filtering Improvements . . . . .	199
New Security Policy Management Support . . . . .	201
Windows Firewall with Advanced Security . . . . .	204
Wired and Wireless Network Policy . . . . .	206
Managing Security Settings . . . . .	208
Summary . . . . .	212
Additional Resources . . . . .	212

<b>8</b>	<b>Auditing. . . . .</b>	<b>213</b>
	Why Audit? . . . . .	213
	How Windows Auditing Works . . . . .	214
	Setting an Audit Policy . . . . .	216
	Audit Policy Options . . . . .	221
	Developing a Good Audit Policy . . . . .	224
	New Events in Windows Server 2008 . . . . .	226
	Using the Built-In Tools to Analyze Events . . . . .	230
	Event Viewer . . . . .	231
	WEvtUtil.exe . . . . .	236
	Summary . . . . .	237

## **Part II   Implementing Identity and Access (IDA) Control Using Active Directory**

<b>9</b>	<b>Designing Active Directory Domain Services for Security. . . . .</b>	<b>241</b>
	The New User Interface . . . . .	241
	The New Active Directory Domain Services Installation Wizard . . . . .	243
	Read-Only Domain Controllers . . . . .	245
	Read-Only AD DS Database . . . . .	246
	RODC Filtered Attribute Set . . . . .	246
	Unidirectional Replication . . . . .	247
	Credential Caching . . . . .	247
	Read-Only DNS . . . . .	249
	Staged Installation for Read-Only Domain Controllers . . . . .	250
	Restartable Active Directory Domain Services . . . . .	251
	Active Directory Database Mounting Tool . . . . .	252
	AD DS Auditing . . . . .	254
	Auditing AD DS Access . . . . .	255
	Active Directory Lightweight Directory Services Overview . . . . .	258
	New Features in Windows Server 2008 for AD LDS . . . . .	261
	Active Directory Federation Services Overview . . . . .	261
	What Is AD FS? . . . . .	262
	What Is New in Windows Server 2008? . . . . .	263
	Summary . . . . .	264
	Additional Resources . . . . .	264

<b>10</b>	<b>Implementing Active Directory Certificate Services. . . . .</b>	<b>265</b>
	What Is New in Windows Server 2008 PKI. . . . .	266
	Threats to Certificate Services and Mitigation Options . . . . .	267
	Compromise of a CA's Key Pair. . . . .	267
	Preventing Revocation Checking. . . . .	268
	Attempts to Modify the CA Configuration. . . . .	271
	Attempts to Modify Certificate Templates . . . . .	272
	Addition of Nontrusted CAs to the Trusted Root CA Store . . . . .	273
	Enrollment Agents Issuing Unauthorized Certificates . . . . .	274
	Compromise of a CA by a Single Administrator . . . . .	275
	Unauthorized Recovery of a User's Private Key from the CA Database. . . . .	277
	Securing Certificate Services. . . . .	277
	Implementing Physical Security Measures . . . . .	278
	Best Practices. . . . .	279
	Summary . . . . .	280
	Additional Resources . . . . .	280

## **Part III Common Security Scenarios**

<b>11</b>	<b>Securing Server Roles . . . . .</b>	<b>285</b>
	Roles vs. Features . . . . .	286
	Default Roles and Features . . . . .	287
	Your Server Before the Roles. . . . .	294
	Default Service Footprint . . . . .	294
	Server Core . . . . .	294
	Roles Supported by Server Core . . . . .	296
	Features Supported by Server Core . . . . .	297
	What Is Not Included in Server Core. . . . .	297
	Tools to Manage Server Roles. . . . .	298
	Initial Configuration Tasks. . . . .	299
	Add Roles and Add Features Wizards . . . . .	299
	Server Manager . . . . .	300
	The Security Configuration Wizard . . . . .	302
	Multi-Role Servers . . . . .	311
	Summary . . . . .	312



<b>12</b>	<b>Patch Management</b>	<b>313</b>
	The Four Phases of Patch Management	313
	Phase 1: Assess	314
	Phase 2: Identify	315
	Phase 3: Evaluate and Plan	318
	Phase 4: Deploy	319
	The Anatomy of a Security Update	320
	Supported Command-Line Parameters	321
	Integrating MSU Files into a Windows Image File	321
	Tools for Your Patch Management Arsenal	322
	Microsoft Download Center	322
	Microsoft Update Catalog	322
	Windows Update and Microsoft Update	323
	Windows Automatic Updating	324
	Microsoft Baseline Security Analyzer	326
	Windows Server Update Services	330
	System Center Essentials 2007	338
	Summary	339
	Additional Resources	340
<b>13</b>	<b>Securing the Network</b>	<b>341</b>
	Introduction to Security Dependencies	344
	Acceptable Dependencies	345
	Unacceptable Dependencies	345
	Dependency Analysis of an Attack	347
	Types of Dependencies	348
	Usage Dependencies	349
	Access-Based Dependencies	349
	Administrative Dependencies	352
	Service Account Dependencies	352
	Operational Dependencies	352
	Mitigating Dependencies	353
	Step 1: Create a Classification Scheme	354
	Steps 2 and 3: Network Threat Modeling	357
	Step 4: Analyze, Rinse, and Repeat as Needed	360
	Step 5: Design the Isolation Strategy	361
	Step 6: Derive Operational Strategy	363
	Step 7: Implement Restrictions	363

	Summary .....	366
	Additional Resources .....	367
<b>14</b>	<b>Securing the Branch Office.....</b>	<b>369</b>
	An Introduction to Branch Office Issues .....	369
	Why Do Branch Offices Matter? .....	370
	What Is Different in a Branch Office? .....	370
	Building Branch Offices .....	371
	Windows Server 2008 in the Branch Office .....	373
	Nonsecurity Features .....	373
	Security Features for the Branch Office .....	376
	Other Security Steps .....	389
	Summary .....	390
	Additional Resources .....	390
<b>15</b>	<b>Small Business Considerations.....</b>	<b>391</b>
	Running Servers on a Shoestring .....	392
	Choosing the Right Platforms and Roles .....	393
	Servers Designed for Small Firms .....	395
	Windows Server 2008 Web Edition .....	395
	Windows Server Code Name “Cougar” .....	395
	Windows Essential Business Server .....	399
	Hosted Servers .....	400
	Virtualization .....	400
	Violating All the Principles with Multi-Role Servers .....	401
	Acceptable Roles .....	402
	Server Components .....	402
	Risk Considerations .....	403
	Edge Server Issues .....	405
	Supportability and Updating .....	406
	Server Recoverability .....	407
	Best Practices for Small Businesses .....	409
	Following Hardening Guidance .....	409
	Policies .....	413
	Vendor Best Practices .....	415
	Remote Access Issues .....	417
	Monitoring and Management Add-ons .....	418
	The Server’s Role in Desktop Control and Management .....	420
	Recommendations for Additional Server Settings and Configurations ....	423

Summary . . . . .	428
Additional Resources . . . . .	428
<b>16 Securing Server Applications . . . . .</b>	<b>431</b>
Introduction . . . . .	431
IIS 7: A Security Pedigree . . . . .	433
Configuring IIS 7 . . . . .	433
Feature Delegation . . . . .	434
TCP/IP-Based Security . . . . .	436
IP Address Security . . . . .	436
Port Security . . . . .	438
Host-Header Security . . . . .	439
Simple Path-Based Security . . . . .	439
Defining and Restricting the Physical Path . . . . .	440
Default Document or Directory Browsing? . . . . .	443
Authentication and Authorization . . . . .	444
Anonymous Authentication . . . . .	445
Basic Authentication . . . . .	446
Client Certificate Mapping . . . . .	447
Digest Authentication . . . . .	450
ASP.NET Impersonation . . . . .	451
Forms Authentication . . . . .	451
Windows Authentication . . . . .	452
Trusting the Server . . . . .	453
Further Security Considerations for IIS . . . . .	455
Summary . . . . .	460
Additional Resources . . . . .	461
<b>Index . . . . .</b>	<b>463</b>

 **What do you think of this book? We want to hear from you!**

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

[www.microsoft.com/learning/booksurvey/](http://www.microsoft.com/learning/booksurvey/)

## Chapter 14

# Securing the Branch Office

— Byron Hynes

**In this chapter:**

**An Introduction to Branch Office Issues**369

**Windows Server 2008 in the Branch Office**373

**Other Security Steps**389

**Summary**390

**Additional Resources**390

In this chapter, we will examine the challenges of a branch office, and some solutions, techniques, and tools to address them. We will start by discussing the characteristics of a branch office, and why they present unique challenges, and then we will look at some of the common infrastructure optimization scenarios that can apply to branch offices. We will go through the features of Windows Server 2008 that support branch offices, and identify those that can particularly help secure branches, focusing on the role of Read Only Domain Controllers (RODCs) and BitLocker Drive Encryption.

## An Introduction to Branch Office Issues

IT security often invokes the image of a well-maintained data center, where IT professionals are constantly striving to improve policies, procedures, settings, and software to protect the physical and knowledge assets in their control. Only a few people can enter the inner sanctum—by “carding in”—to find orderly arrangements of neatly placed computers, efficiently humming along while being securely watched.

Many of our readers—you—strive to build this sort of environment. But, did you realize that about one-third of IT budgets are spent on branch offices, or remote locations? Between one-quarter and one-third of servers running Windows Server software are installed in what we call a branch office.

Branch offices are found in many diverse environments. I worked with a customer in the fast-food industry who had a Windows server in every one of thousands of restaurants, nationwide. A colleague of mine did an early Active Directory design and deployment project with domain controllers in each one of 800 branches of a major European bank. Branch offices can include retail stores, medical facilities, hotels—perhaps even the check-in counter

where you drop off your child for daycare, or the elementary school office where the secretary enters daily attendance information.

## Why Do Branch Offices Matter?

Branch offices are not going away anytime soon. Quite the opposite, actually. Branches are where the vast majority of business is won or lost for a corporation; branches are where services are delivered for nonprofits and government agencies. In addition to online services, branches are where source data is collected and interpreted, and where more savvy consumers are demanding that decisions can be made by local representatives.

Unfortunately, a number of characteristics can be limiting or even negative for the branch office.

## What Is Different in a Branch Office?

Branch offices come in many different configurations, but most share the following traits:

- **Remotely connected over a WAN** While network speeds continue to increase, most branch offices depend on an externally controlled network, such as a leased line, frame relay connection, or shared fiber circuit. Some branch offices are connected only over the public Internet, using a virtual private network (VPN). Remember that when you depend on a third party, such as a telephone or network company, you have no control over what happens to your data on that network.
- **Reduced physical security** Servers in branch offices are rarely accompanied by the same level of physical security found in a corporate data center. I hope that your server is not stuck under a receptionist's desk in a public area, or sitting on a shelf in a restroom, but I have seen both.
- **Lack of local skilled IT personnel** In a branch office, particularly a small one, you often find that an employee with little or no formal IT skill "inherits" the care and feeding of your server in the branch. This might be the business manager (or highest-ranking employee on site), the local tech enthusiast, or even just the staff member who is "always there" and never in a meeting.
- **Distance** As well as not being staffed with IT professionals, a branch office is more often than not geographically far from IT support. It may be impossible to get one of your own analysts or technicians on-site in less than a day or two.
- **Reduced infrastructure** Unlike the data center, with its precise climate control, redundant power supplies, and multiple communication paths, branch offices may not be engineered to the same level of fault tolerance—both in terms of IT systems and in terms of civil infrastructure, such as power and communications.

Branch offices face growing pressures, including cost and performance pressures, pressure to remain secure and in compliance with growing laws and regulations, and the pressure to be agile and responsive to business needs. For example, branch offices face the high costs of

maintaining complex, disparate, and often nonintegrated hardware sets, coupled with the high cost of bringing in IT support when needed, either from the data center or perhaps by subcontracting expensive local support agencies. Of course, branch office managers—and certainly the home office management team—are aware of the threats posed by data breaches, attacks against the system, and the difficulty of recovering from a disaster and protecting that locally collected data. (After all, why go after Jesper’s well-hardened servers—you know, the ones he keeps in his data center and has guarded by men with guns, 24 hours a day—if a much less secure server is sitting in the local branch.)

But even with all of that, branch offices are expected to have and use more and more information as a “point of service,” where data is collected, analyzed, and used to deliver immediate results, all while being integrated across the company. I remember opening a bank account as a teenager where the ledger was still kept by hand—and of course, that account could only be accessed at that particular branch. I do not expect that many banks would be able to compete using that kind of operation today! (And, just so you do not think I am too old, I should add that I walked down the street to a competitor with computers and multi-branch services.)

On the whole, a branch office represents a simple challenge for the consummate IT professional. All you have to do is secure remote data and access; protect systems; provide secure connectivity with reduced on-site support, simple backups, and efficient use of hardware and bandwidth—while also improving your infrastructure, delivering new capabilities quickly, and establishing a platform for the future and maintaining compliance. (Whew!)

IDC describes it this way:

*Branch locations often are looking for high levels of flexibility and autonomy in implementing IT solutions. However, expanding corporate requirements call for centralized management, enhanced security, and regulatory compliance.*

Source: **IDC White Paper, Addressing Operational Efficiencies in Branch Office, May 2006**, located at [http://download.microsoft.com/download/6/d/0/6d032455-bf07-42ac-b006-ee0e4c8ab606/idc\\_branch\\_whitepaper.pdf](http://download.microsoft.com/download/6/d/0/6d032455-bf07-42ac-b006-ee0e4c8ab606/idc_branch_whitepaper.pdf)

## Building Branch Offices

A number of design scenarios can address the branch office situation. Basically, they range on a continuum from one or more gargantuan servers in the branch office to “no servers in the branch office, do it all remotely.” As you can imagine, each of these possible solutions has strengths and weaknesses.

To leave myself some room in this chapter to talk about securing Windows Server 2008 in the branch office, I am only going to present a brief overview of design approaches. Some of these approaches are very common; others are only occasionally used. Some are becoming more popular as lower costs and new technologies become more commonplace. And many branch offices have a combination of elements from more than one of the following options.

- **Virtualized server in the branch office** A server capable of running a virtual server image for each workload provides maximum flexibility and configurability—and agility—with a solution that allows all workloads and services to be run off of a single, physical server computer. This option is best where there are numerous stand-alone servers that could be consolidated into a single unit. Services are run in-house in order to allow 100 percent uptime and functionality even when the wide area network (WAN) or VPN is offline. By managing only one server, you can gain some centralized management and data backup.
- **Single server** Using one server offers the benefits of a server in the branch office, but without the cost and complexity of supporting virtualization and server consolidation. In this case, services that must be constantly available or that require the lowest possible latency can be run from within the remote office, while others are centralized to the data center. You must strike a balance between reliance on WAN uptime, remote management, centralized backup, and local responsiveness.
- **Branch office appliances** Branch office appliances strive to provide a complete solution that is easy to deploy and configure out-of-the-box. These appliances typically provide WAN acceleration and HTTP compression, making it easier to centralize workloads such as storage and databases. The branch office appliance may come preloaded with some line-of-business (LOB) applications or other services to allow the branch to continue to operate during a WAN outage. Appliances can be designed to connect to a WAN or to use the Internet as VPN appliances.
- **Secure centralization** In this sort of design, the server is removed from the branch location and all workloads are centralized. Application virtualization (such as the sort provided by Microsoft SoftGrid Application Virtualization) is used to allow LOB applications to be run from the data center but executed on the local desktop, reducing the burden of deploying and managing updates to those applications that are virtualized. A security appliance, intelligent firewall, or gateway enables secure connectivity (including packet filtering and VPN access) to the data center.
- **No infrastructure** In this case, the branch office simply has no servers or significant networking hardware. Everyone relies on network connectivity to the data center to enable all remote office functionality. Essentially, everyone is a network client. Remote office employees either exist on the same corporate network as the head office using a WAN, or they connect via VPN to the data center to access applications, or all branch office users are treated as Internet users and applications are delivered via secured Internet protocols. This reduces remote infrastructure deployment to a bare minimum and eliminates remote server management.

Microsoft offers a number of products and solutions for the branch office, as well as extensive infrastructure optimization (IO) guidance to help you select and build an effective and secure remote or branch office infrastructure. For the rest of this chapter, we will focus on branch office features and enhancements in Windows Server 2008, primarily those that are directly

related to securing the branch office. For more information about branch offices in general (or using Windows Server products in branch offices), visit <http://technet.microsoft.com/en-us/branchoffice/default.aspx>.

## Windows Server 2008 in the Branch Office

Improving the situation in branch offices was one of the main goals during the development of Windows Server 2008. Features in Windows Server 2008 address the concerns of a branch office in three areas: cost control, security, and business agility. Table 14-1 summarizes the features designed in Windows Server 2008 to overcome branch office challenges.

**Table 14-1 Windows Server 2008 Branch Office Challenges and Solutions**

Challenge	Requirement	Windows Server 2008 Features
Cost control	Reduce the cost of managing and supporting remote offices (including making most efficient use of network links).	Server Core installation option Read-Only Domain Controller (RODC) Server Message Block (SMB) 2.0 Data Protection (Backup) Windows Server Virtualization
Security	Improve security of data and access.	BitLocker Drive Encryption Read-Only Domain Controller (RODC) Server Message Block (SMB) 2.0
Agility	Provide a flexible infrastructure that maximizes IT investment.	Server Message Block (SMB) 2.0 TCP/IP redesign

## Nonsecurity Features

I want to spend most of this discussion covering security features, but other features deserve a mention too, because it is often difficult—and usually counterproductive—to look at security in complete isolation. By understanding how all of the pieces fit together, you can be more effective—and that leads to being more secure.

In a very pragmatic sense, it is also a really good idea to strive to keep your network solutions cost-effective, agile, reliable, and available. When your solutions fail to meet end users' needs (or perceived needs), your end users (and especially management) will seek workarounds or shortcuts. These shortcuts are *rarely* secure. This is not to say that these users are being malicious. They will, however, go around you or your security when what you have put in place does not do what they need, or what they think they need.

### Server Core Installation Option

Server Core is a minimal server installation option for Windows Server 2008 that contains a subset of executable files and makes available only a few server roles. Server Core runs on either 32-bit or 64-bit architectures.



I consider Server Core to be a security feature because it reduces the attack surface in the server. Only the binaries need to support the role and the base operating systems. This means that generally fewer processes are running. But Server Core is also a cost-control feature because it reduces maintenance and management requirements.

The Server Core installation option installs only a subset of the executable files and supporting dynamic-link libraries (DLLs). Specifically, only those features that are required by nine specific server roles are installed. Components not installed include Graphical User Interface (GUI), the .NET Framework Common Language Runtime (CLR), the Windows Explorer user interface, and Internet Explorer. Because there is no GUI interface, administrators must access all of these services through a local command shell, either remotely from a management server or workstation (with a remote command shell or with a remote tool, such as an MMC snap-in), or by using the new remote management feature called WS-Management, or by using the Windows Management Interface (WMI).

One of the biggest single benefits of a Server Core installation is a much reduced need for updating. While updates are the bane of an IT professional's existence in the data center, updating remote and branch offices has its own special kind of pain. Based on comparisons with Windows Server 2003, Microsoft estimates that less than 60 percent of updates would have applied to a Server Core installation than would be needed for a full installation of Windows Server, if that kind of installation existed for Windows Server 2003. Server Core is described in more detail in Chapter 12, "Securing Server Roles."

## Hyper-V (Windows Server Virtualization)

Windows Server 2008 Hyper-V, formerly called Windows Server Virtualization, is a virtualization platform designed to provide the flexibility through a dynamic, reliable, and scalable platform capabilities. You can also use a single set of integrated management tools to manage both physical and virtual server resources. Hyper-V is included in most Windows Server 2008 licenses, but you may need to download it from Microsoft separately.

A full discussion of virtualization is outside the scope of this chapter. But because many branch office situations will benefit from Server Virtualization, you should read more about it on the Web at <http://www.microsoft.com/windowsserver2008/virtualization/default.aspx>.

## Complete Redesign of TCP/IP Stack

Sometimes called the Next Generation TCP/IP stack, the improved networking stack in Windows Server 2008 and Windows Vista has some direct benefits to the branch office. By improving network communication between servers in the data center and the branch office, and between remote clients and centralized services, you can maximize the use of WAN links.

From a security point of view, you should be aware of the following aspects of the new TCP/IP functionality:

- Expanded IPsec integration and easier IPsec management tools.
- TCP/IP includes an integrated filtering platform. Windows uses this platform for Windows Firewall and IPsec, but other applications and vendors can also make use of the Windows Filtering Platform (WFP).

Both of these issues are discussed in Chapter 5, “Windows Firewall(s),” and Chapter 13, “Managing Security Dependencies to Secure Your Network.” As well, the redesign of TCP/IP is discussed extensively in TechNet online (<http://technet.microsoft.com/en-us/network/bb545475.aspx>) and *Windows Server 2008 TCP/IP Protocols and Services* by Joseph Davies (Microsoft Press, 2008).

## Server Message Block

Continuing with the theme of connectivity and protocols, Windows Server 2008 includes a new remote file sharing protocol, Server Message Block 2.0 (SMB 2.0). SMB is the protocol generally used between Windows computers, such as Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008.

SMB 2.0 greatly improves the scalability of SMB 1.0, increasing the number of open files and allowed shares. The protocols have been enhanced to reduce the “chattiness” that makes file sharing on a WAN sometimes painful. Real-world testing has shown improvements with SMB 2.0 copying large files up to 35 times faster than with SMB 1.0. However, SMB 2.0 benefits only really appear when communicating between Windows Server 2008 computers or between Windows Server 2008 and Windows Vista clients. SMB 2.0 is not available separately for older Windows operating systems.

To learn more about the WAN performance improvements in SMB 2.0, watch the TechNet webcast “Wide Area Network Performance Improvements in Windows Server 2008” at <http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?culture=en-US&EventID=1032348651&CountryCode=US>.

## Data Protection—Windows Server 2008 Server Backup

Remember that security includes keeping data available and being able to recover from disasters. Windows Server Backup uses the Volume Shadow Copy Service (VSS) and block-level backup technology to back up your servers, locally or remotely, with less downtime. Support has also been added for backing up to optical media (DVD) and to another file server.

## Security Features for the Branch Office

Two more major components of Windows Server 2008 have a direct impact on securing your branch offices: Read-Only Domain Controller (RODC) and BitLocker Drive Encryption.

### RODC

RODC is a new feature in Active Directory Domain Services (AD DS) in Windows Server 2008. Please refer to Chapter 9, “Designing Active Directory Domain Services for Security,” for an overview of AD DS features and information about using and installing RODCs. In this chapter, I want to focus on the security implications of an RODC in a branch office.

**RODC Read-Only Database, Replication, and Group Memberships** As the name suggests, RODCs are read-only copies of the AD DS database. This means that they require only unidirectional replication for Active Directory, as well for the File Replication Service (FRS) and Distributed File System Replication (DFSR).

One-way replication imparts a security benefit. Any compromise or other issue that introduces poisoned data into the RODC’s local copy of the AD DS database cannot be replicated back to the rest of the organization from the affected RODC. This is certainly a mitigation that can help stop a local problem from becoming a global problem! On the other hand, be aware that if malware, attacks, or other issues cause you to have a corrupt, or “owned” local domain controller—even a read-only one—you still have a big problem to deal with!

Additional steps have also been taken to minimize the problems that could potentially be caused by a rogue RODC. Each RODC has its own, unique KrbTGT account for the Key Distribution Center (KDC), allowing the system to know when a ticket has been issued by an RODC (and which one) and when it has been issued by a normal, writable DC. This is a form of *cryptographic isolation*, a phrase you will sometimes hear used in conjunction with RODC discussions.

One-way replication brings benefits in terms of designing your replication topology and controlling replication traffic, as well. Bridgeheads and hubs do not have to poll the RODC for changes. The RODC performs normal inbound replication for AD DS and FRS and any DFSR changes.

Because the RODC is a member of the domain, sometimes it has a legitimate need to write to Active Directory. However, it does not write to the local database copy, but will instead connect to a writable DC, just like a workstation. The RODC computer account is a workstation account, so it has very limited rights to write to AD DS—again to minimize any damage to the enterprise AD DS if the RODC is compromised. Because they are “workstations” in this sense, RODC computer accounts are not members of the Enterprise Domain Controllers (EDC) or Domain Domain Controllers groups.

**Database Contents and Credential Caching** With the exception of account passwords and attributes specifically added to the filtered attribute set, an RODC holds all the AD DS objects and attributes that a writable domain controller holds.

Local applications that request read access to the domain directory information can obtain access directly from the RODC, while Lightweight Directory Access Protocol (LDAP) applications that request write access receive an LDAP referral response. This referral response directs them to a writable domain controller, normally in a hub site.

In the domain database, each security principal—user, computer, or iNetOrgPerson—has a set of up to 10 passwords or secrets, collectively called credentials. An RODC does not store these credentials, except for its own computer account and the special krbtgt account for each RODC. The RODC is advertised as the Key Distribution Center (KDC) for its site, which should normally be the branch office in which it is located. When the RODC issues and signs a ticket-granting ticket (TGT), it uses its own krbtgt account and keys, which are different from the krbtgt account shared by the KDCs on all writable domain controllers in the domain.

The first time a user attempts to authenticate to an RODC, the RODC sends the request to a writable domain controller at the hub site. If the authentication is successful, the RODC also requests a copy of the appropriate credentials. The writable domain controller recognizes that the request is coming from an RODC and consults the Password Replication Policy that is in effect for that RODC.

The Password Replication Policy determines whether the credentials are allowed to be replicated and stored on the RODC. If so, a writable domain controller sends the credentials to the RODC, and the RODC caches them for future use. After the credentials are cached on the RODC, the next time that user attempts to log on, the request can be directly serviced by the RODC until the credentials change.

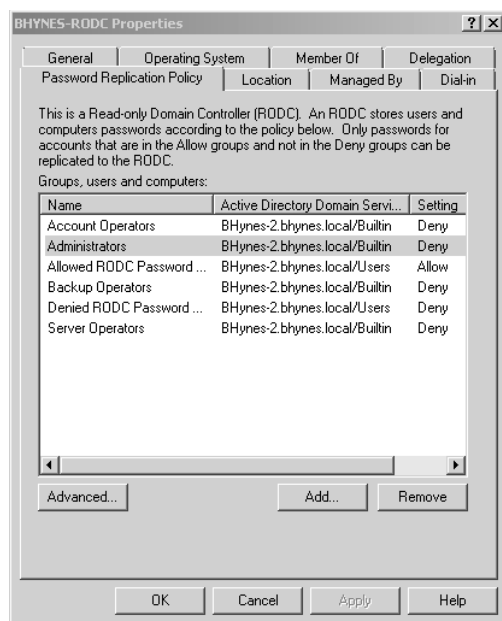
Obviously, for this to work the RODC has to know whether it is likely to have a copy of the credentials. To avoid needless lookups, the RODC checks the signature on various requests. If a TGT has been signed with its own krbtgt account, the RODC immediately recognizes that it has a cached copy of the credentials. Conversely, if another DC has signed the TGT, the RODC will always forward requests.

The key to limiting risk by installing RODCs in branch offices is correctly using the Password Replication Policy to control which credentials are cached. By default, no user credentials will be cached on an RODC, but that is an inefficient design. If you think about most domains with a branch office, you realize that even in a large branch (say 100 users), those users are a tiny percentage of users in the domain. If you have 20,000 users in the domain, that is one half of one percent.

Because only a few domain users need to have credentials cached on any given RODC, use the Password Replication Policy to specify which groups of users can even be considered for caching. By limiting RODC caching to only users who are frequently at that branch office, you can reduce the potential exposure. You can—and should—also explicitly block the caching of credentials for high-value accounts. By denying the caching of accounts for Domain Admins, for example, you guarantee that Domain Admin credentials will never be stored on the RODC in that branch office. This is where the real security benefit comes in over Windows Server 2003,

where you had no option but to have a local copy of every account in every branch office. This is a huge security improvement.

You access the Password Replication Policy by selecting the Properties of the RODC computer object. In Figure 14-1, you can see that only accounts in a group representing that Branch Office are allowed to be cached, and high-value credentials are explicitly denied.



**Figure 14-1** An RODC's property sheet showing its Password Replication Policy.

Let us consider for a moment that the unthinkable has happened and your RODC is stolen. The evildoer mounts the AD DS database and attempts to retrieve passwords using a commonly available, umm, “security research” tool. However, instead of seeing more and more passwords appear as the password cracking progresses, the tool only shows empty or blank passwords for almost all accounts.

In the past, if your DC was stolen, you would really have no choice but to reset all of the passwords in the domain—a formidable task if you have thousands of users. However, in this case, you only need to deal with the specific accounts that have already been cached on that RODC. To be clear: With an RODC, you know exactly which passwords have been cached. You can check which ones have been replicated to the RODC by looking at the Password Replication Policy dialog box. Initially, only the computer itself and the special KRBTG account have passwords stored locally, as you can see in Figure 14-2. After clients begin to authenticate to the RODC, additional passwords may also be stored, as shown in Figure 14-3.

You can also determine which users have attempted to authenticate to the RODC, but whose passwords have not been allowed to be cached. For example, notice in Figures 14-2 and 14-3

that no password has been cached for the Administrator account. However, as shown in Figure 14-4, the administrator has logged on in the site served by the RODC.

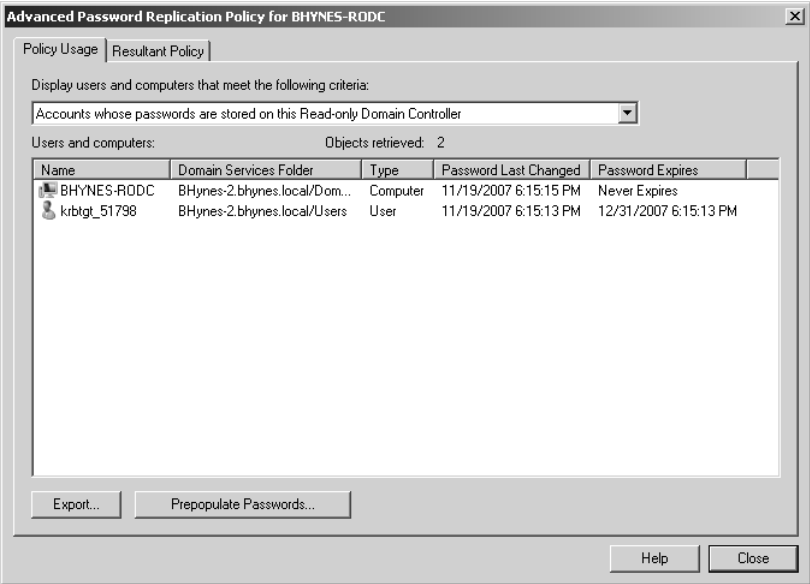


Figure 14-2 Initially, only two accounts have passwords stored on the RODC.

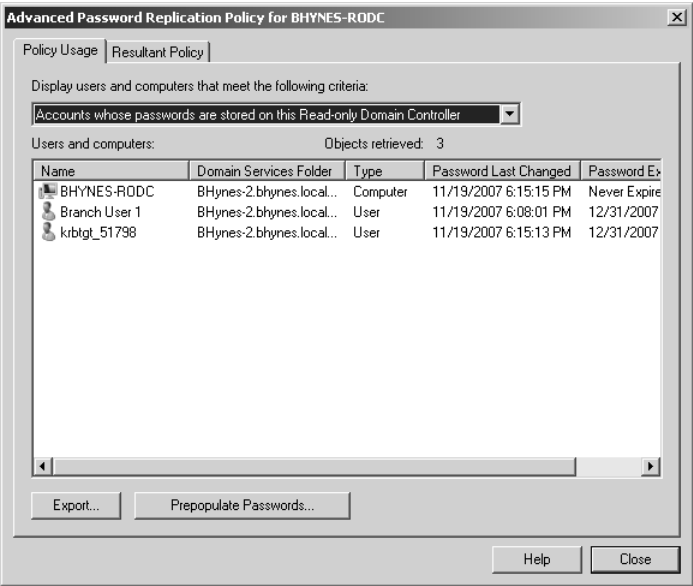
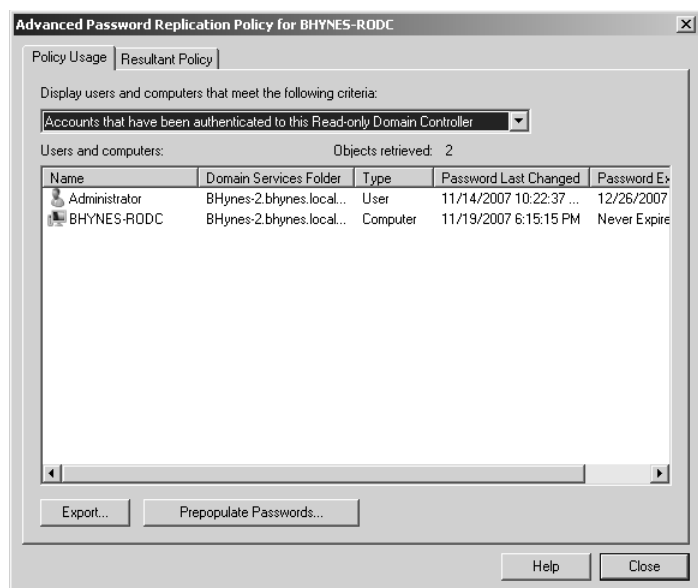
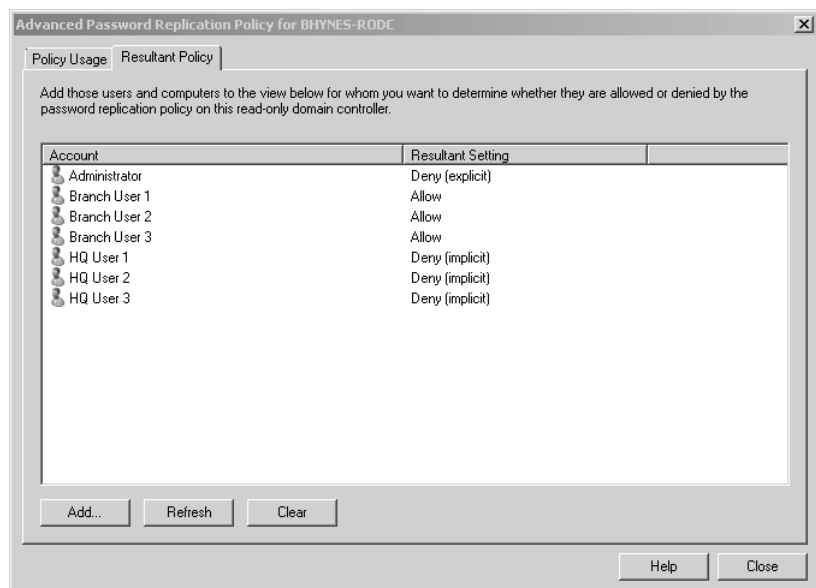


Figure 14-3 You can store additional passwords on the RODC.

Finally, as shown in Figure 14-5, you can model which accounts will be allowed or not allowed to have passwords cached on the RODC.

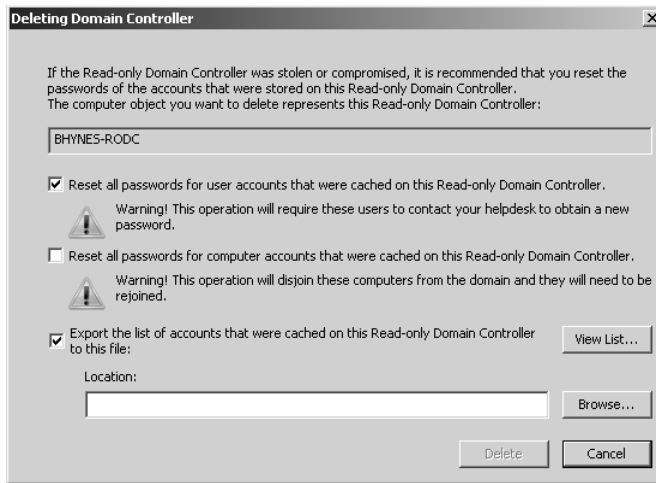


**Figure 14-4** Users who have authenticated to the RODC, but have not had passwords cached.



**Figure 14-5** Using the Resultant Policy page to model password caching.

We have made it much easier to delete missing domain controllers, including RODCs, with a simple interface that can remove the departed RODC from the domain (no more metadata cleanup needed!) and also automatically reset the potentially compromised passwords. When you start to delete the computer object representing an RODC, you see the dialog pictured in Figure 14-6.



**Figure 14-6** Removing an RODC that cannot be brought online from AD DS.

You should also read ahead to the section on BitLocker Drive Encryption. By using BitLocker on the Windows operating system volume of the RODC, you can prevent the thief from even being able to access the local copy of the AD DS database—which, at a minimum, buys you time to reset passwords in an orderly fashion.

**Administrative Role Separation** With Role Separation you can delegate the local administrator role of an RODC computer to any domain user without granting that user any rights to the domain itself or to other domain controllers. In Windows Server 2003, DCs didn't have a local administrator; if you could administer a DC, you could administer the whole domain.

Administrative Role Separation can allow a local branch user to log on to an RODC and perform maintenance work on the server, such as upgrading a driver, without allowing that user to log on to any other domain controller or manage the domain.

**RODC Benefits** RODCs provide a way to deploy domain controllers more securely in a branch office location because they are designed to be placed in locations that require rapid, reliable, and robust authentication services but that might also have a security limitation that limits or prevents deployment of a writable domain controller. With an RODC, organizations can mitigate risks with deploying a domain controller in locations where physical security cannot be guaranteed.

The RODC feature is clearly designed for branch offices, but it is an integral part of AD DS as well. Please review Chapter 9 for information about installing an RODC, using the RODC filtered attribute set, and configuring read-only DNS.

## BitLocker Drive Encryption

BitLocker Drive Encryption is a component of the operating system in Windows Vista Enterprise Edition and Windows Vista Ultimate Edition, and it is also included as a feature in all



editions of Windows Server 2008. You may already be familiar with the need to protect data on client hard drives, but that need can be just as important on servers, particularly in a branch office.

According to Forrester, data breaches are expensive: “The cost of a single, significant security breach may run into millions or even billions of dollars.” (“Calculating the Cost of a Security Breach,” Khalid Kark, April 10, 2007: <http://www.forrester.com/Research/Document/Excerpt/0,7211,42082,00.html>) and, unfortunately, they are also common: “34% of respondents experienced at least one personal data breach.” (“Aligning Data Protection Priorities with Risk,” Jonathan Penn, April 13, 2006: <http://www.forrester.com/Research/Document/Excerpt/0,7211,39257,00.html>)

Most IT professionals are well aware of the risk of a user’s laptop being left in a taxi or stolen. Hopefully, you are not likely to leave a production server in a taxi, but have you considered what would happen if your servers were stolen? I worked with a military customer once who told me that his organization had equipped domain controllers with C4 explosive charges because they were deployed “in theater” and would be destroyed rather than risk authentication data falling into enemy hands. Now, your risk is probably not the same as those on the battlefield, but there is always some risk, and it is not just hypothetical. A colleague of mine (okay, it was Jesper), was involved with a customer’s organization that did have a thief back a truck into and through the wall of their building to steal their servers.

BitLocker gives you another tool to help mitigate the risk at the level you need. I hope, however, that you are thinking beyond the data center. Here are some contrasting examples from my work experience:

- I visited one particular customer whose data center happened to be in a 100-year-old former sanatorium. The servers were all behind two-foot-thick stone walls, and staffed 24 hours a day. It would be hard to steal those servers.
- I volunteered at a large youth event, where the “data center” was in a tent. Servers strung around several hundred acres lost connectivity whenever someone plugged a kettle into the same electrical outlet as the fiber-optic repeater.

Lest anyone dismiss my second example, let me point out that both servers held confidential personal information including health information about clients or participants—and both were where they *needed to be to meet the particular business demand*.

So what is BitLocker Drive Encryption and how can it help secure the data on your servers? BitLocker performs two functions:

- BitLocker encrypts all data stored on the Windows operating system volume (and configured data volumes). This includes the Windows operating system, hibernation and paging files, applications, and data used by applications.
- BitLocker is configured by default to use a Trusted Platform Module (TPM) microchip to help ensure the integrity of early start-up components (components used in the earlier stages of the start-up process), and locks any BitLocker-protected volumes so that they remain protected even if the computer is tampered with when the operating system is not running.

**BitLocker Configuration in Windows Server 2008** In Windows Server 2008, BitLocker is an optional component that must be installed before it can be used. (In Server Manager, optional components are called *features*.) To install BitLocker, select it in Server Manager or type the following at a command prompt: **ServerManagerCmd -install BitLocker-restart**.

Installing BitLocker on a production server means giving consideration to a few points. BitLocker has two optional components (OCs) included with Windows Server 2008. The BitLocker OC is used to protect volumes on that particular server. There is also a remote administration OC called RSAT-BitLocker that installs the binary files and command-line scripts required to manage BitLocker on remote servers. (RSAT stands for Remote Server Administration Tool.) If you install or remove the BitLocker feature using Server Manager, both OCs are installed or removed. If you only want to install the remote tool, you must use either the **pkgmgr** command or the **ocsetup** command. Because Server Manager is not supported with the Server Core installation option, you must use **pkgmgr** or **ocsetup** to install BitLocker on Server Core.

Because BitLocker uses a filter driver for encryption and decryption, installing or removing BitLocker requires a restart of the computer. Installing the RSAT-BitLocker component alone does not. After the component is installed, you can use the command-line tool, `manage-bde.wsf`, or Control Panel to enable BitLocker on particular volumes.

BitLocker is different from existing technologies like EFS because once you turn BitLocker on, it is automatic, transparent, and includes the entire volume. (Note that BitLocker is fully compatible with EFS, and you can use them both together to mitigate different risks. Active Directory Rights Management Service, or AD RMS, adds the third part of Microsoft's data encryption strategy. EFS and RMS are outside the scope of this chapter.)

BitLocker does require that a computer be configured with multiple volumes (partitions). A computer will start from the active partition, sometimes called the system partition or system volume. The operating system is installed on a second volume, which Windows Server 2008 documentation usually calls the Windows OS volume, but older documentation refers to as the boot partition. (Yes, for those keeping score: You never did boot from the boot partition and no Windows system files are on the system partition.)

The active partition is not encrypted, but the Windows OS volume is. In other words, BitLocker encrypts everything written to a protected volume: code, data, and temporary files.

BitLocker's full-volume encryption protects against offline attacks—the kind of attacks that are mounted by trying to bypass the operating system. It is absolutely essential to understand that BitLocker does not protect a *running* operating system. Once the Windows OS Volume has been unlocked at start-up, BitLocker continues to encrypt and decrypt sectors on the fly—whenever an application or the operating system itself reads or writes data on a protected volume—but it has no more protection function to perform. Instead, BitLocker helps protect you against offline attacks such as having the disk (or entire server) stolen.

Without BitLocker, it is a trivial exercise to take the disk out of a server and put it in another computer to bypass NTFS permissions and similar defenses. With BitLocker, though, nothing on that disk can be read in another computer, unless you have the required recovery password to unlock the volume. It is also true that files protected by RMS and EFS will also not be easily read, but BitLocker extends protection to the entire volume, including files that cannot be protected by RMS or EFS (such as the Active Directory database or the registry).

### **Direct from the Source: Automatically Unlock Data Volumes**

In Windows Server 2008, Microsoft added support for fixed data volumes to BitLocker. Along with that comes the ability to automatically unlock (auto-unlock) any encrypted data volumes. To do this, BitLocker stores keys for encrypted data volumes (the “auto-unlock keys”) in the system registry, where they are retrieved by BitLocker to unlock the volume.

It is very important to protect the auto-unlock keys, since they can be used to decrypt the volume. Therefore, these keys are always themselves encrypted before being stored in the registry. They are encrypted by using a new key called the Auto-Unlock Master Key (AMK). The AMK is very similar to the FVEK. The FVEK is used to encrypt the data on the volume, while the AMK is used to encrypt the data in the registry. Like the FVEK, the AMK is encrypted by the OS Volume’s VMK, which explains the necessity of enabling BitLocker first on the OS Volume before it can be enabled on any data volume.

With this design, you can safely enable BitLocker on a data volume and set it to auto-unlock (which is the by default) without waiting for the OS Volume to be fully encrypted.

Also, since decrypting the OS Volume causes the AMK to be deleted and, therefore, the auto-unlock keys in the registry to become unusable, if you decrypt the OS volume, we also force decryption of all mounted data volumes that are set to auto-unlock.

*Narendra S. Acharya*

*Software Design Engineer in Test (SDET)*

*System Integrity, Core OS Division*

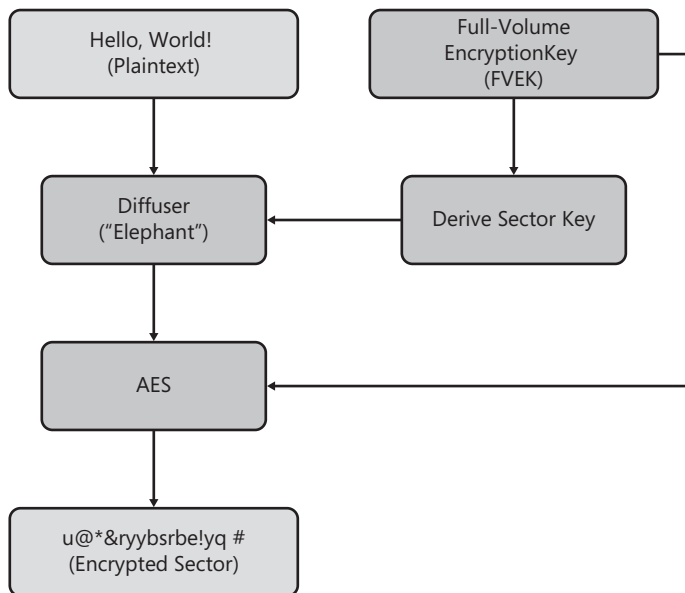
**BitLocker Encryption Algorithms and Keys** BitLocker uses the Advanced Encryption Standard (AES) algorithm with a 256-bit key space. However, with the default setting only 128 bits of the key are used. For stronger encryption, the key length can be increased to 256-bit keys using Group Policy or the BitLocker Windows Management Instrumentation (WMI) provider. As with all encryption, stronger encryption and longer keys result in more processing power being used. (To take effect, any changes to the encryption settings need to be made before BitLocker is turned on for a volume.)

Before data is passed to the AES algorithm, it is run through two separate diffuser steps. A *diffuser* is a complex cryptographic algorithm with a simple purpose. The diffusers ensure that any change (even only one bit) made to the plaintext will result in the entire block being

changed in the encrypted ciphertext. This makes it harder, if not impossible, to guess keys by making changes in the plaintext to see predictable output in the ciphertext.

With BitLocker, each sector in the volume is encrypted individually. Part of the encryption key is calculated from the sector number itself. This means that two sectors with the same unencrypted data will also result in two totally different encrypted blocks being written to the disk. This also makes it harder to discover the keys by encrypting known pieces of information.

One of the developers of the algorithm, and a respected cryptographer who worked on BitLocker, Niels Ferguson, presented and published a paper on the details of the BitLocker encryption algorithm. It is available on the book's companion CD-ROM and online at <http://www.microsoft.com/downloads/details.aspx?familyid=131dae03-39ae-48be-a8d6-8b0034c92555&displaylang=en>: "AES-CBC + Elephant Diffuser: A Disk Encryption Algorithm for Windows Vista." A simplified overview is shown in Figure 14-7.



**Figure 14-7** Simplified overview of BitLocker encryption algorithm.

As I mentioned, each sector is encrypted uniquely, with part of the key being derived from the sector number. The symmetric encryption key that is used for the bulk of the encryption is called the Full-Volume Encryption Key (FVEK). The FVEK is never revealed to a user or to an administrator. If the FVEK were compromised, security best practices would dictate that everything it encrypted would need to be decrypted and re-encrypted with a new key. Because we could be dealing with very large quantities of data, that would be a time-consuming process (during which noticeable performance degradation could occur). Instead, the FVEK is kept as a very closely guarded secret, and the system works with another key called the Volume Master Key (VMK). The VMK is used to encrypt the FVEK. The encrypted copy of the FVEK is written to the volume metadata. (It can also be backed up as part of a binary key package to AD DS.) This is not like leaving the key under the mat—it is more like leaving the key in a safe bolted to

two tons of concrete, and then hidden under the mat. In addition, if the VMK is somehow compromised, you can re-encrypt the FVEK with a new VMK very quickly.

To decrypt sectors, the system needs to get the FVEK. To get the FVEK, the system needs to get the VMK. The VMK is also stored in the volume metadata, and it is also never written to disk without being strongly encrypted itself.

The VMK can be encrypted by any number of key protectors or authenticators. The default key protector is the computer's Trusted Platform Module (TPM), as discussed in the following sections. You can combine the TPM with a numeric PIN or a partial key stored on a USB key or both. By adding a PIN or USB requirement, you are introducing a form of two-factor authentication.

If the computer does not have a compatible TPM, you can configure BitLocker to store a key protector completely on a USB Flash Drive (although this does not provide any boot integrity checking, as discussed later). The VMK is also encrypted with a 48-digit recovery password that can be backed up to AD DS, stored in a database, or printed to be used for emergency recovery.

Finally, in a case where you want to disable BitLocker but not fully decrypt the drive, BitLocker uses a *clear key* key protector. The clear key is very much like putting the key to the door under the mat. The VMK is encrypted with a new key, but that key is stored in plaintext on the volume. This is effective for operations that require BitLocker to be deactivated, such as some kinds of upgrades, but avoids the time required to decrypt and re-encrypt the volume. However, because the VMK could be somewhat easily discovered in this state, you should not leave BitLocker in this disabled state for any longer than necessary.

**BitLocker Start-up** At start-up, all BitLocker-protected volumes are locked and cannot be used, even to start the operating system. Early start-up code in the Boot Manager and Windows Loader looks for an appropriate key protector by querying the TPM, checking the USB ports, or, if necessary, prompting the user for a PIN or a recovery password. Finding a key protector lets Windows decrypt the VMK, which decrypts the FVEK. At this point, the disk is unlocked and the BitLocker filter driver decrypts the data stored on disk as each sector is read.

**BitLocker Integrity Checking** When a server starts, the components used early in the process need to be unencrypted so that they can be used in start-up. If an attacker could change the code in the earliest start-up components, compromising a system is much, much easier. This is the basis of many rootkits. Once a system is compromised this way, secrets such as passwords can be much more easily obtained.

In the case of a system protected by BitLocker, a compromise of the earliest components could lead to the disclosure of the VMK or FVEK and render the protection of BitLocker useless, even though data on the disk is encrypted.

If the computer has a compatible TPM, BitLocker can use integrity checking functionality to help prevent this sort of attack. With a TPM, each time the computer starts, each of the early start-up components—such as the BIOS, the master boot record (MBR), the boot sector, and

the boot manager code—examines the code about to be run, calculates a hash value, and stores the value in specific registers called platform configuration registers (PCRs) in the TPM. Once a value is stored in a PCR, the value cannot be replaced or erased unless the system is restarted.

A TPM can encrypt data (in this case, the VMK) and tie that encryption to specific PCR values, which is called *sealing* a key to the TPM. Once sealed, only that specific TPM can decrypt that key, and the TPM will decrypt the key only if the current PCR values match the values specified when the key was sealed.

By default, BitLocker seals keys to the PCRs that record the Core Root of Trust Measurement (CRTM), the BIOS and any platform extensions, option ROM code, MBR code, the NTFS boot sector, and the boot manager. If any of these items change unexpectedly, the TPM will not decrypt its key protector, and BitLocker will not be able to unlock the volume. This prevents the volume from being accessed or decrypted.

By default, BitLocker is configured to look for and use a TPM. You can use Group Policy or a local policy setting to allow BitLocker to work without a TPM and store keys on an external USB Flash Drive, but without a TPM, BitLocker cannot verify system integrity.

**BitLocker in the Branch Office** “That’s all well and good,” you might be thinking, “and sure, it helps with laptops. But what does it have to do with my server in a branch office?” I’m glad you asked.

In several specific scenarios BitLocker can help immensely with servers, particularly those not housed in the central data center. These include:

- **Reducing exposure to malware, especially rootkits.** Most rootkits and other malware that can do serious damage on your servers require a restart to install. By using a TPM module and BitLocker’s integrity checking, the server will not start if the early start-up components have been manipulated. (Windows Code Integrity features take over protecting the operating system against unauthorized changes after BitLocker unlocks the volume.) It is true that this could result in a denial of service because the server will not restart, but it is generally better to be stopped than to be running with active malware on a production server.
- **Theft of a server.** Thieves target laptops and mobile devices because they are often convenient targets. While some thieves steal them because they may contain some interesting bits of information, most laptop theft is for the hardware, not the infinitely more valuable data that is on them—information. But a server or its disks can be the mother lode to a serious thief. A domain controller could contain secrets for thousands of users (see the section on RODCs!); a file server could be filled with your company’s intellectual property; a database server could have reams and reams of personally identifiable information—handy for identity theft and fraud, to name but two. Note that to effectively mitigate against the risk of the entire server being stolen, using the default of TPM protection only will not be enough.

- **Theft of a disk.** It is often much easier to remove a single disk than to steal the entire server. Most server disks are swappable, so it only takes a moment for someone to remove one. Like a server, a disk contains valuable information and should be protected.
- **Shipping a server (or disk) to a remote location.** In many cases, servers are first provisioned centrally or large amounts of data need to be shipped to a remote server. In either case, you can enable BitLocker on the volume at the data center, and then ship the volume to the remote location. In the case of an entire server, it can be configured to require a start-up PIN. For a single volume, all key protectors except the recovery password can be removed. Then, after authorized personnel have possession of the server or disk at the destination, the PIN or recovery password can be provided by telephone, fax, or e-mail. Once the server is in production, if desired, you can remove the PIN requirement or even decrypt the volume. If the disk or server is lost or stolen in transit, the data cannot be accessed.
- **Secure decommissioning.** At some point, a server or disk needs to be removed from service. It is absolutely essential that no server disk with company data leave your possession with that data still readable. Most processes that remove confidential data from disk drives are time consuming, costly, or result in the permanent destruction of the hardware. Instead of removing the data after the fact, BitLocker helps ensure that confidential data is not stored on disk in a risky way in the first place. Because everything written to the disk is encrypted, you can permanently render the data completely inaccessible by destroying all copies of the encryption keys. The hard disk itself is completely unharmed and can be reused. Removal and destruction of the keys contained in the volume metadata is instantaneous and can be performed locally or remotely by an administrator. The format utility in Windows Vista and Windows Server 2008 deletes the volume metadata and overwrites those sectors to securely delete any BitLocker keys. (Note that you cannot use the format utility from Windows versions earlier than Windows Vista to achieve the same result.)

**BitLocker Caveats and Trade-offs** As you consider using BitLocker on your servers, bear a few things in mind.

Remember that BitLocker protects against certain specific threats—from offline attacks. It is imperative that other security controls, such as strong passwords, remain in place. Likewise, BitLocker does not prevent the destruction of data or the denial of service. Backups are still essential. In fact, if you do not take care to ensure the accessibility of the recovery passwords, BitLocker could prevent you from accessing your data! We recommend using BitLocker's built-in ability to back up recovery information to AD DS. For more information about backing up recovery information, see “Configuring Active Directory to Back Up Windows BitLocker Drive Encryption and Trusted Platform Module Recovery Information” at <http://technet2.microsoft.com/WindowsVista/en/library/3dbad515-5a32-4330-ad6f-d1fb6dfcdd411033.mspx?mfr=true>.

In Windows Server 2008 and Windows Vista SP1, BitLocker uses a cryptographic signature to check for certain types of deliberate attacks. If one of these attacks occurs, the cryptographic

signature is invalid, and BitLocker will lock out the recovery password as well as routine key protectors. This scenario will only occur if the attacker has physical possession of the volume or computer. If you regain possession of the volume, you will need to use the BitLocker Repair Tool and a backup copy of the FVEK, as well as the recovery password. Therefore, you should ensure that these items are backed up using the AD DS system or the WMI provider.

Also keep in mind that BitLocker is an optional feature on Windows Server 2008. Because the encryption and decryption operations are implemented in a filter driver, you cannot use BitLocker until you install the feature, as described earlier in this chapter. Note, however, that installing or removing BitLocker requires restarting the server.

BitLocker does not support clusters. If you configure servers in failover clusters, you cannot use BitLocker to protect shared volumes.

BitLocker—like all encryption products and technologies—incurs a performance hit. In most user scenarios, this performance is not noticeable, and can be measured at well less than 5 percent. However, if your server is performing intensive disk operations or is very heavily loaded, you may need to take this into consideration in capacity planning.

Security is often a matter of trade-offs. One significant trade-off to make with regards to BitLocker is whether to require user intervention at start-up. By default, BitLocker operates using the TPM as a key protector and, providing that the integrity validation completes successfully, BitLocker will unlock the Windows operating system volume without user intervention. However, this means that a thief who takes the entire server can also turn it on without any interference from BitLocker.

To mitigate this risk, use the TPM with a PIN, with a USB Flash Drive (called a *startup key*), or both. This increases security tremendously, but it also means that a server cannot automatically restart. (Leaving a start-up key in the server all the time would be a foolish idea.) Because servers are normally running this may not be a problem—until a power failure results in the branch being down because the one manager who had the PIN is on vacation.

My recommendation, in most cases, is to use a TPM plus PIN, but to ensure that there is an operational procedure that describes who knows the PIN, how to use it, and how to obtain the PIN from central support if needed. This also requires that any planned restarts (such as for an operating system upgrade or update) are scheduled when someone with the PIN is on-site. Only your organization can make the call about which is the more important risk: potential additional downtime or potential theft of the server.

## Other Security Steps

I believe you need to invest in two other areas to protect your branch office servers: physical security and user education.

While features such as RODC and BitLocker help mitigate risk, a bad guy having physical possession of your server is still a big deal. Even if he cannot gain access to the data, he can



still prevent your users from gaining access to it. Reasonable investments in physical security also increase the availability of services.

I continue to hear stories of cleaning staff unplugging servers, unnecessary water damage, and accidental shutdowns. Use locked closets or cabinets. Plan for UPS protection. Ensure proper ventilation. For large enterprises, this may be obvious—but then again, in a big firm, do you know the condition of every server in the truck shop or out on the plant floor?

Also invest in user education. Explain the importance of security and how to treat both the physical and data assets in their care. This may be more important than ever in small branch offices with no dedicated IT staff, let alone compliance and security officers.

## Summary

Windows Server 2008 has been designed from the ground up to support branch offices, and introduces tools to make securing them easier than ever. The RODC and BitLocker features are key weapons in your arsenal of protection.

## Additional Resources

- Windows BitLocker Drive Encryption Frequently Asked Questions
- BitLocker Drive Encryption Technical Overview
- *Data Encryption Toolkit for Mobile PCs*
- BitLocker Drive Encryption Glossary
- BitLocker Drive Encryption (from Changes in Functionality from Windows Server 2003 with SP1 to Windows Server 2008)
- BitLocker Drive Encryption Step-by-Step Guide for Windows Server 2008
- Windows BitLocker Drive Encryption Step-by-Step Guide (for Windows Vista)
- Windows BitLocker Drive Encryption Design and Deployment Guides
- *Configuring Active Directory to Back Up Windows BitLocker Drive Encryption and Trusted Platform Module Recovery Information*
- BitLocker Drive Encryption Events and Errors
- AD DS: Read-Only Domain Controllers (<http://technet2.microsoft.com/windowsserver2008/en/library/ce82863f-9303-444f-9bb3-ecaf649bd3dd1033.mspx?mfr=true>)
- Step-by-Step Guide for Read-Only Domain Controllers (<http://technet2.microsoft.com/windowsserver2008/en/library/ea8d253e-0646-490c-93d3-b78c5e1d9db71033.mspx?mfr=true>)
- Branch Office Infrastructure Solution for Microsoft Windows Server 2003 Release 2 (<http://www.microsoft.com/technet/solutionaccelerators/branch/default.mspx>)