MCSE Windows® 2000 Network Security Design

0-7357-0984-X

by Roberta Bragg

Warning and Disclaimer: This book is designed to provide information about Windows 2000. Every effort has been made to make this book as complete and accurate as possible, but no warranty or fitness is implied. The information is provided on an as-is basis. The authors and New Riders Publishing shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

Misprint	Correction
Page 7 Hardware and Software You ll Need • Windows 2000 Server and Professional • A server and a workstation computer on the Microsoft Hardware Compatibility List • Pentium 90MHz (or better) processor • 600MB (or larger) hard disk • VGA (or Super VGA) video adapter and monitor • Mouse or equivalent pointing device • CD-ROM drive • Network interface card (NIC) or modem connection to Internet • Presence on an existing network, or use of a two-port (or more) miniport hub to create a test network • Internet access with Internet Explorer 4 (Service Pack 1) or later • 24MB of RAM (32MB recommended) • Windows NT Option Pack recommended • Microsoft SQL Server 6.5 (or better) optional • Microsoft SNA Server optional	Should be: **Windows 2000 server and/or Advanced Server:** • 133 MHz or higher Pentium-compatible CPU. • 256 megabytes (MB) of RAM recommended minimum (128 MB minimum supported; 4 gigabytes (GB) maximum]. (Will load on 64 MB RAM, but will be slow) • 2 GB hard disk with a minimum of 1.0 GB free space. (Additional free hard disk space is required if you are installing over a network.) **Windows 2000 Professional:** • 133 MHz or higher Pentium-compatible CPU. • 64 megabytes (MB) of RAM recommended minimum; more memory generally improves responsiveness. • 2GB hard disk with a minimum of 650MB of free space.
Page 163 Active Directory and Security The Security Accounts Manager (SAM) is not required but is present to provide compatibility where necessary with down-level clients.	Should be: The Security Accounts Manager (SAM) database is not required but is present to provide compatibility where necessary with down-level clients.
Page 165 Trusts 1st Paragraph: Windows NT domains could share resources by creating one-way trusts between domains. 4th Paragraph: External trusts are one-way trusts that exist between a domain in your forest and another domain outside the forest.	Should be: 1st Paragraph: Windows NT domains share resources with other Windows NT domains by creating one-way trusts between domains. 4th Paragraph: External trusts are one-way trusts that exist between a domain in your forest and another domain outside the forest and can be created between two domains in separate forests.
Page 167 Domains 2nd Paragraph: Windows NT domains were limited by the number of user accounts.	Should be: Windows NT domains limit the number of user accounts that can exist in a domain.
Page 168 2nd Paragraph: Security settings can be modified by	Should be: Security settings can be modified also by setting

setting Local Computer Policy.	Local Computer Policy.
Page 169 *Notes* (table column) Uses recommended security settings for all security areas except files, folders and registry keys. This enables SMB packet signing. Uses settings for network communications. Applies security for optional components, such as DNS and DHCP.	Should be: Secure: Uses recommended security settings for all security areas except files, folders and registry keys. This template enables SMB packet signing. High Security: Uses settings for network communications. Optional Components: Applies security for optional components, such as DNS and DHCP.
Page 173 Bulleted list • Event Log Policies • Restricted Group Policies • System Services Policies • Registry Policies • File System Policies	Should be: • Event Log Policies • Restricted Groups • System Services Policies • Registry • File System
Page 183 Forest-Wide Operations Master Roles Two operations master roles are forest-wide that is, only one of each is necessary in the forest.	Should be: Two operations master roles are forest-wide that is, only one of each exists in the forest.
Page 184 Domain-Wide Operations Master Roles Just as some operations master roles are forest-wide, three roles are domain-wide. Each new user, group, or computer in a domain gets a unique security ID. This ID is partially composed of a unique domain security ID	Should be: Just as some operations master roles are forest-wide, three roles are only domain-wide. Each new user, group, or computer in a domain gets a unique security ID (SID). The SID is partially composed of a unique domain security ID
Page 187 Servers It can also exist as an application server, a file and print server, a Web server, or a RAS server.	Should be: It can also exist as an application server, a file and print server, a Web server, or Routing and Remote Access Services (RRAS) server.
Page 192 RAS Server instances of RAS servers on pgs 192-193	Should be: RRAS Server instances should be RRAS servers
Page 205 Automated Install To install, many computers develop automated installation. Part of the preparation for automated installs is to create a distribution folder that contains the Windows 2000 installation files as well as any device driver and other files needed. During Windows 2000 installation, the appropriate (server defltsv.inf) file is parsed (On the installation CD-ROM the file is compressed with the .in extension.)	Should be: To install many computers, develop automated installation. Part of the preparation for automated installs is to create a distribution folder that contains the Windows 2000 installation files as well as any device drivers and other files needed. During Windows 2000 installation, the appropriate default template file is parsed (On the installation CD-ROM the file is compressed with the .in_ extension.)
Page 207 Table 4.15 **Parameter** **Explanation** /CFG filename This is the path of the security template. (Without this, any configuration in the database is used.)	Should be: This is the path of the security template. (Without this, the configuration in the database is used.)
Page 208 **Key Terms**	Should be:

• Security Configuration and Analysis Template • security groups • RAS server	• Security Configuration and Analysis • security groups • RRAS server
Page 209 **Table 4.17 Exercise 4.2** **Template Answers** *Baseline Template* hisecdc	Should be: **Table 4.17 Exercise 4.2** **Template Answers** *Baseline Template* hisecws
Page 210 **Review Questions #12** Identify which security template you would use for securing the ITS RAS server and what changes	Should be: Identify which security template you would use for securing the ITS RRAS server and what changes
Page 213 #11 and #12 instances of RAS servers	Should be: RRAS servers
Page 214 First paragraph A user can easily find a printer or a service within the forest by querying the active direction.	Should be active directory
Page 214 #5 Security templates can be applied directly to the local computer or to a Group Policy object.	Should be: Security templates can be applied directly to the local computer or imported into a Group Policy Object (GPO).
Page 215 #12 Instances of RAS server Page 216 #11 Instances of RAS server	Should be: RRAS server
Page 222 The section titled Special Permissions discusses folder permissions in detail.	Should be: The section titled File and Folder Advanced Permissions discusses folder permissions in detail.
Page 233 **Table 5.1** File Path What Is? Permission	Should be: File Path Description Permission
Page 241 Instances of RAS	Should be: RRAS
Page 243 2nd Paragraph To specify who can change a user s password, use the Delegation of Authority Wizard.	Should be: To specify who can change a user s password, use the Delegation of Authority Wizard, or use the security tab on the object s property pages.
Page 251 **Answers to Exam Questions** #2 C, D.	Should be: C (only)
Page 252 #7 A, B, C, D.	Should be: A, B, C. (not D)
Page 268 NOTE Use the Domain Security Policy to set audit policy for local databases on servers and professional systems joined in the domain.	Should be: for local user databases on servers
Page 270 Managing the Log Log settings are specified in the Group Policy Object\Computer Configuration\Windows Settings\Event Log folder.	Should be: Log settings are specified in the Group Policy Object\Computer Configuration\Windows Settings\Security Settings\Event Log folder.
Page 288 NOTE Distribution groups are lists; they can be used for mail.	Should be: Distribution groups are lists; they can be used for mail, but not for resource access.
Page 289 2nd Paragraph If the server is promoted to a domain controller, the Administrator account becomes a member in the following groups:	Should be: If the server is promoted to be the first domain controller in the forest, the Administrator account becomes a member in the following groups:
Page 293 **Group Strategies**	Should be:

If you are familiar with Windows NT group strategies, you probably learned about AGLP, which reminded you to add users to Global groups you can expand this strategy to UGUDLP.	If you are familiar with Windows NT group strategies, you probably learned about AGLP, which reminded you to add user Accounts to Global groups you can expand this strategy to AGUDLP.
Page 294 4th Paragraph --the child OUs can have their own groups and cannot administer groups created in the parent OU.	Should be: --the child OUs can have their own groups, yet Administrators of the child OU cannot administer groups created in the parent OU.
Page 297 **Administrators** When that computer joins a domain, that user has no rights or privileges in the domain until he or she is assigned some. **Backup Operators** Members of the Backup Operators group can back up and restore all domain controllers using Windows Backup. They do not use the Backup Operators group, but they create two new groups one for each operation.	Should be: **Administrators** When that computer joins a domain, that user has no rights or privileges in the domain until he or she is given a domain account and rights in the domain. **Backup Operators** Members of the Backup Operators group can back up and restore all files on computers that are joined in the domain. They do not use the Backup Operators group, but they create two new groups one for each operation, and assign the backup, or restore rights to each group as appropriate.
Page 299 **Replicator** The Replicator group is created to hold a user that will be used to log on to the file replication service.	Should be: **Replicator** The Replicator group is created to hold a user that will be used to log by the replication service.
Page 302 2nd Bullet & 1st Paragraph DNS Update Proxy	Should be: DNSUpdateProxy
Page 302 • Everyone • Interactive • Authenticated Users • Creator Owner • Network • Dialup • Anonymous Users	Should be: • EVERYONE • INTERACTIVE • AUTHENTICATED USERS • CREATOR OWNER • NETWORK • DIALUP • ANONYMOUS USERS
Page 308 (heading) **SIDS, ACLS, and RIDS**	Should be: **SIDS, DACLS, and RIDS**
Page 352 **Step by Step 8.1** #4 Use the browse button to move the different Group Policies. (It is here that you select the policy you want to edit.) Then return to the Local Computer Policy.	Should be: Use the browse button to find and select the policy you want to edit.
Page 353 #7 Expand the Policy tree, and select System under User Configuration\Administrative Templates.	Should be: Expand the Policy tree, and select an item.
Page 356 Bulleted List • Policies are reapplied throughout the day. • Local Computer Policy is applied. • Any site policies are applied. • Any domain policies are applied. • OU policies are applied. • If OUs are nested, each inner nested OU	Should be: • Policies are reapplied throughout the day. Policy is processed in the following order: 1. Local Computer Policy is applied. 2. Any site policies are applied. 3. Any domain policies are applied. 4. OU policies are applied.

Group Policy is applied. - At each level, all applicable Group Policies are applied in the order specified by the administrator. - Finally (excluding the Local Computer Policy), the policy closest to the user or group is also applied.	5. If OUs are nested, each inner nested OU Group Policy is applied. - At each level, all applicable Group Policies are applied in the order specified by the administrator.
Page 358 2nd Paragraph His Windows 98 computer does not have the directory Services client and so can only do LM authentication.	Should be: The account OU enforces a policy that requires NTLMv2 authentication. Since the Windows 98 computer does not have the directory Services client it can only do LM authentication.
Page 401 1st Paragraph You can export EFS private keys for protection.	Should be: You can export EFS private keys to back them up.
Page 403 3rd Paragraph Instead, to remove the possibility	Should be: Entire paragraph replaced with: To disable EFS, either delete the policy or delete the recovery agent certificate for the policy. If no recovery agent exists, there can be no file encryption.
Page 429 **Kerberos Components** - Authentication Server-- In Windows 2000, this is implemented as a service: the Authentication Service (AS). - Ticket-Granting Server-- In Windows 2000, this is implemented as the Ticket-Granting Service.	Should be: - Authentication Server-- In Windows 2000, this is implemented as a part of the KDC Service. - Ticket-Granting Server-- In Windows 2000, this is implemented as the Ticket-Granting Service, a part of the KDC Service.
Page 477 2nd Paragraph Windows 2000 using Kerberos and request certificates.	Should be: Windows 2000 using Kerberos and request tickets.
Page 510 1st Paragraph CryptoAPI is Microsoft s application programming interface that provides functions for encryption, description, and digital signing.	Should be: CryptoAPI is Microsoft s application programming interface that provides functions for encryption, decryption, and digital signing.
Page 519 2nd Paragraph under the Table the Certificate Services Web Enrollment Support is added.	Should be: the Certificate Services Web Enrollment Support is added during installation.
Page 543 4th Paragraph Microsoft standards include the support of ITU X.509 version 3 and version 1 certificate formats..	Should be: Microsoft standards include the support of ITU X.509 version 2 and version 3 certificate formats..
Page 565, list of objectives Under the main objective "Design Windows 2000 network services security" a subobjective is missing from the list.	Should be added to end of subobjective list: - Design Windows 2000 Terminal Services security.
Page 588 **Security for Non-Windows 2000 Clients** Instead, make these DHCP servers members of the DNSUPdateproxy group.	Should be: Instead, make these DHCP servers members of the DNSUpdateProxy group.
Page 588 **WARNING** Warning! Do not make a DHCP Server a Member of DNSUPDAT if the DHCP Server .	Should be: Warning! Do not make a DHCP Server a Member of DNSUpdateProxy if the DHCP Server .

This errata sheet is intended to provide updated technical information.
Spelling and grammar misprints are updated during the reprint process,
but are not listed on this errata sheet.