

MCTS Self-Paced Training Kit (Exam 70-640): Configuring Windows Server® 2008 Active Directory® (2nd Edition)

Dan Holme, Nelson Ruest, Danielle Ruest, Jason Kellington

ISBN: 978-0-7356-5193-7

First printing: June, 2011

To ensure the ongoing accuracy of this book and its companion content, we've reviewed and confirmed the errors listed below. If you find a new error, we hope you'll report it to us on our website: www.microsoftpressstore.com/contact-us/errata.

Page	Location	Description	Date corrected
	Throughout the book	<p>Author note:</p> <p>Dear readers: In the practice exercises of the 70-640 Training Kit, you log on to domain controllers with user accounts that are not members of Domain Administrators or the domain's Administrators group. Therefore, you must give all user accounts the right to log on locally to the domain controllers in your practice environment. In the Training Kit, we use a shortcut to provide this right: We guide you to add Domain Users to the Print Operators group, which has the right assigned by default. Unfortunately, in limited circumstances, this shortcut can lead to problems with certain exercises. Therefore, instead of adding Domain Users to the Print Operators group, follow the steps in the article, "Grant a Member the Right to Logon Locally," at http://technet.microsoft.com/en-us/library/ee957044(WS.10).aspx to grant the Allow Logon Locally right to the Administrators and Domain Users groups. If you will use Remote Desktop Services to connect to the domain controller—rather than logging on locally—grant the Allow Logon Through Remote Desktop Services right. This is for the practice environment only. In a production environment, you should not grant users the right to log on to domain controllers.</p>	
	Throughout the book	<p>Author note:</p> <p>Dear readers: Please note that you should NOT copy and paste commands from the PDF or other eBook format of the Training Kit. PDFs and eBook files contain hidden characters such as nonbreaking spaces and line breaks that will cause unexpected errors. The exercises and sample commands have been tested by TYPING commands as shown.</p>	
10	First bulleted item, penultimate sentence	<p>Reads:</p> <p>...the domain is considered to have two trees.</p> <p>Should read:</p> <p>...the forest is considered to have two trees.</p>	2/17/2012

Page	Location	Description	Date corrected
29	Exercise 2, step 2	<p>The following paragraph should be added below the code block in step 2.</p> <p>Should read: If you receive an error, check that your network interface is called "Local Area Connection" by typing netsh interface show interface. Replace "Local Area Connection" in the commands shown above with the correct name of your network connection.</p>	2/17/2012
29	Exercise 2, steps 4 and 7	<p>Reads: 4. Restart by typing shutdown -r -t 0.</p> <p>Should read: 4. Restart by typing shutdown /r /t0.</p> <p>Reads: 7. Restart by typing shutdown -r -t 0, and then log on again as Administrator.</p> <p>Should read: 7. Restart by typing shutdown /r /t0, and then log on again as Administrator.</p>	11/18/2011
29	Exercise 2, step 12	<p>Reads: 12. Type oclist and confirm that the DNS server role is installed.</p> <p>Should read: 12. Type oclist more and—using the space bar to page through—confirm that the DNS server role is installed.</p>	11/22/2013
30	Exercise 3, step 3, code block	<p>Reads: dcpromo /unattend /replicaOrNewDomain:replica /replicaDomainDNSName:contoso.com /ConfirmGC:Yes /UserName:CONTOSO\Administrator /Password:* /safeModeAdminPassword:P@ssword</p> <p>Should read: dcpromo /unattend /replicaornewdomain:replica /replicaDomainDNSName:contoso.com /ConfirmGC:Yes /UserName:Administrator /userDomain:Contoso /Password:* /safeModeAdminPassword:P@ssword</p>	11/18/2011
31	Question 2	<p>Reads: 2. SERVER02 is running Server Core. It is already configured with the AD DS role. You want to add Active Directory Certificate Services (AD CS) to the server. What must you do?</p> <p>Should read: 2. SERVER02 is running Server Core. It is already configured with the AD DS role. You want to add Active Directory Federated Services (AD FS) to the server. What must you do?</p>	9/23/2011

Page	Location	Description	Date corrected
52	Paragraph before step 9, last sentence	<p>Reads: The DNS name of your Active Directory domain will always be available, because a suffix and cannot be removed.</p> <p>Should read: The DNS name of your Active Directory domain will always be available as a UPN suffix and cannot be removed.</p>	2/17/2012
85	Last paragraph	<p>Reads: In addition, make sure that the Domain Users group is a member of the Print Operators group, which can be found in the Builtin container. This allows all sample users in the practice domain to log on to the SERVER01 domain controller. This is important for the practices in this training kit, but you should not allow users to log on to domain controllers in your production environment, so do not make Domain Users members of the Print Operators group in your production environment.</p> <p>Should read: In this and other practices in this training kit, you will log on to the domain controller with user accounts that are not a member of Domain Administrators or the domain's Administrators group. Therefore, you must give all user accounts the right to log on locally to the domain controllers in your practice environment. Follow the steps in the article, "Grant a Member the Right to Logon Locally," at http://technet.microsoft.com/en-us/library/ee957044(W.S.10).aspx to grant the Allow Logon Locally right to the Administrators and Domain Users groups. If you will use Remote Desktop Services to connect to the domain controller—rather than logging on locally—grant the Allow Logon Through Remote Desktop Services right. This is for the practice environment only. In a production environment, you should not grant users the right to log on to domain controllers.</p>	2/17/2012
91	Fourth bulleted item	<p>Reads: DSMove Moves an object to a new container or OU.</p> <p>Should read: DSMove Moves an object to a new container or OU or renames an object.</p>	2/17/2012
107	Penultimate paragraph	<p>Reads: For example, to get help, including examples, about the New-ADGroupMember cmdlet...</p> <p>Should read: For example, to get help, including examples, about the Get-ADGroupMember cmdlet...</p>	2/17/2012

Page	Location	Description	Date corrected
113	Paragraphs after Tip reader aid	<p>Reads:</p> <p>To create a new OU for Contractors in the User Accounts OU, type the following command: <code>md "ou=Contractors"</code></p> <p>Md is an alias for the New-Item cmdlet. In the example, a number of defaults were used to create the result: a new OU named Contractors in the User Accounts OU.</p> <p>Should read:</p> <p>To create a new OU for Contractors in the User Accounts OU, type the following: <code>md "ou=Contractors"</code></p> <p>Md is an alias for the mkdir function, which itself is a wrapper around the New-Item cmdlet. The syntax is familiar to anyone who has used Command Prompt. But the result is a new OU named Contractors in the User Accounts OU.</p>	7/27/2012
122	Exercise 5, step 2, code block	<p>The space before @contoso.com should be removed from the second and fourth lines of code.</p> <p>Reads:</p> <pre>New-ADUser -Path "ou=User Accounts,dc=contoso,dc=com" -Name "Linda Mitchell" -SAMAccountName "linda.mitchell" -UserPrincipalName "linda.mitchell @contoso.com" New-ADUser -Path "ou=User Accounts,dc=contoso,dc=com" -Name "Scott Mitchell" -SAMAccountName "scott.mitchell" -UserPrincipalName "scott.mitchell @contoso.com"</pre> <p>Should read:</p> <pre>New-ADUser -Path "ou=User Accounts,dc=contoso,dc=com" -Name "Linda Mitchell" -SAMAccountName "linda.mitchell" -UserPrincipalName "linda.mitchell@contoso.com" New-ADUser -Path "ou=User Accounts,dc=contoso,dc=com" -Name "Scott Mitchell" -SAMAccountName "scott.mitchell" -UserPrincipalName "scott.mitchell@contoso.com"</pre>	2/17/2012

Page	Location	Description	Date corrected
122	Exercise 4, steps 5 and 8	<p>In step 5, the code line should be changed.</p> <p>Reads: New-Item -Name "ou=Employees" -ItemType organizationalUnit</p> <p>Should read: New-Item -Name "ou=New Hires" -ItemType organizationalUnit</p> <p>Step 8 should be changed.</p> <p>Reads: ...confirm that the Employees and Contractor...</p> <p>Should read: ...confirm that the Employees, Contractors and New Hires...</p>	9/23/2011
133	Code block and paragraph after numbered list	<p>In the code block, the fifth square-bracketed element should be changed.</p> <p>Reads: [-dn DisplayName]</p> <p>Should read: [-display DisplayName]</p> <p>In the first full sentence of the paragraph after the code block, the following change should be made.</p> <p>Should read: Each parameter, -display, for example...</p>	2/17/2012
137	Fourth paragraph	<p>Reads: To reset a user's password by using Windows PowerShell, use the Set-ADUser cmdlet's -AccountPassword parameter, as explained in Lesson 2.</p> <p>Should read: To reset a user's password by using Windows PowerShell, use the Set-AccountPassword cmdlet, as explained in Lesson 2.</p>	2/17/2012
156	Figure 4-5	<p>Screenshots in figure show the incorrect group name.</p> <p>Reads: Sales</p> <p>Should read: ACL_Sales Folders_Read</p>	
159	"Understanding Group Types" section, line 4	<p>The following text should be removed: —they do not have SIDs—</p>	2/17/2012

Page	Location	Description	Date corrected
163	Third bulleted list item, second sentence	<p>Reads: Additionally, a universal group can be used to manage resources—for example, to assign permissions—anywhere in the forest.</p> <p>Should read: Additionally, a universal group can be used to manage resources—for example, to assign permissions—anywhere in the forest and in trusting forests.</p>	2/17/2012
192	Step 2	<p>Reads: 2. Right-click the group's name and choose Properties.</p> <p>Should read: 2. Right-click the OU and choose Properties.</p>	2/17/2012
200	Question 1	<p>Reads: 1. Your company is conducting a meeting for a special project. The data is particularly confidential. The team is meeting in a conference room, and you have configured a folder on the conference room computer that grants permission to the team members. You want to ensure that team members access the data only while logged on to the computer in the conference room, not from other computers in the enterprise. What must you do?</p> <p>Should read: 1. Your company is conducting a meeting for a special project. The data is particularly confidential. The team is meeting in a conference room, and you have configured a folder on the conference room computer that grants permission to the team members. The folder is a subfolder of a shared folder to which all employees have access. You want to ensure that team members access the data only while logged on to the computer in the conference room, not from other computers in the enterprise. What must you do?</p>	2/17/2012
203	Practice 2, third line of code	<p>Reads: dsmod group "CN=User Accounts,OU=Groups,DC=contoso,DC=com" - addmbr</p> <p>Should read: dsmod group "CN=All Users,OU=Groups,DC=contoso,DC=com" - addmbr</p>	9/23/2011
219	Second bulleted list, first bulleted item	<p>Reads: ...for example, CN=Client Computers,...</p> <p>Should read: ...for example, OU=Client Computers,...</p>	11/18/2011

Page	Location	Description	Date corrected
221	Paragraph before bulleted list, last sentence	<p>Reads: Some of these objects were created in practices in earlier chapters, and some are new for this chapter.</p> <p>Should read: Some of these objects were created in practices in earlier chapters. If the objects already exist, move them to the locations indicated.</p>	2/17/2012
227	"Creating Computers with DSAdd" section	<p>The contents of this section are inaccurate and should be replaced with the following.</p> <p>Should read: The DSAdd command was used in previous chapters to create objects in Active Directory.</p> <p>To create computer objects, simply type dsadd computer ComputerDN where ComputerDN is the distinguished name (DN) of the computer, such as "CN=Desktop123,OU=Desktops,DC=contoso,DC=com". If the computer's DN includes a space, surround the entire DN with quotation marks.</p> <p>The DSAdd Computer command can take the following optional parameters after the DN parameter:</p> <ul style="list-style-type: none"> • -samid ComputerName • -desc Description • -loc Location <p>If you type DSAdd Computer /?, the help text for the command states the following:</p> <p>If you enter multiple values, the values must be separated by spaces (for example, a list of computer distinguished names).</p> <p>This is not accurate. You cannot use the DSAdd Computer command to add multiple computers with a single command.</p>	2/17/2012
234	First code block, first line	<p>Reads: OU=Computers</p> <p>Should read: CN=Computers</p>	2/17/2012

Page	Location	Description	Date corrected
349	Step 8	<p>Reads: Explore the settings that were discovered on SERVER01, but do not change any settings, on the following pages of the wizard: Select Server Roles, Select Client Features, Select Administration And Other Options; Select Additional Services; and Handling Unspecified Services.</p> <p>Should read: Explore the settings that were discovered on SERVER01, but do not change any settings, on the following pages of the wizard: Select Server Roles, Select Client Features, Select Administration And Other Options; Select Additional Services; and Handling Unspecified Services.</p>	9/23/2011
394	Last two paragraphs	<p>Reads: Three settings are related to account lockout. The first of these settings, Account Lockout Threshold, determines the number of invalid logon attempts permitted within a time specified by the second of these settings, Account Lockout Duration. If an attack results in more unsuccessful logons within that time frame, the user account is locked out. When an account is locked out, Active Directory denies logon to that account, even if the correct password is specified.</p> <p>An administrator can unlock a locked user account by following the procedure you learned in Chapter 3. You can also configure Active Directory to automatically unlock the account after a delay specified by a third setting, the Reset Account Lockout Counter After policy setting.</p> <p>Should read: Three settings are related to account lockout. The first of these settings, Account Lockout Threshold, determines the number of invalid logon attempts permitted within a time specified by the second of these settings, Reset Account Lockout Counter After. If an attack results in more unsuccessful logons within that time frame, the user account is locked out. When an account is locked out, Active Directory denies logon to that account, even if the correct password is specified.</p> <p>An administrator can unlock a locked user account by following the procedure you learned in Chapter 3. You can also configure Active Directory to automatically unlock the account after a delay specified by a third setting, the Account Lockout Duration policy setting.</p>	9/23/2011
411	Last paragraph, sixth sentence	<p>Reads: Replication is one way (from a writable domain controller to a RODC).</p> <p>Should read: Replication is one way, from a writable domain controller to the RODC.</p>	2/17/2012

Page	Location	Description	Date corrected
412	First full sentence	<p>Reads: Finally, RODCs, unlike writable DCs, have a local administrators group.</p> <p>Should read: Finally, RODCs, unlike writable DCs, have some local groups, most notably a local Administrators group.</p>	2/17/2012
413	Step 2	<p>Reads: 2. Right-click the name of the forest and choose Properties.</p> <p>Should Read: 2. In the console tree, right-click the root node, Active Directory Domains And Trusts [Server Name], and then click Properties.</p>	2/17/2012
425	First paragraph, fourth sentence	<p>Reads: ...Service Configuration Manager (SCM)...</p> <p>Should read: ...Service Control Manager (SCM)...</p>	2/17/2012
466	"DNS Devolution" section, third paragraph, first sentence	<p>Reads: Note that devolution will not work if a global suffix list is configured through Group Policy or if the Append parent suffixes of the primary DNS suffix check box is selected in the Advanced TCP/IP Settings for the IPv4 or IPv6 properties of a network connection.</p> <p>Should read: Note that devolution will not work if a global suffix list is configured through Group Policy or if the Append parent suffixes of the primary DNS suffix check box is not selected in the Advanced TCP/IP Settings for the IPv4 or IPv6 properties of a network connection.</p>	11/18/2011
486	Last paragraph, third sentence	<p>Reads: For example, if you are using site-local addresses in your network, you might type fe80::/64 as the address scope.</p> <p>Should read: For example, if you are using link-local addresses in your network, you might type fe80::/64 as the address scope.</p>	11/18/2011
513	Step 2	<p>Reads: 2. Copy the contents of the \Sources\Adprep folder...</p> <p>Should read: 2. Copy the contents of the Support\Adprep folder...</p>	2/17/2012

Page	Location	Description	Date corrected
514	Second and third numbered lists, both steps 2	<p>First step 2 reads: 2. Copy the contents of the \Sources\Adprep folder...</p> <p>Should read: 2. Copy the contents of the \Support\Adprep folder...</p> <p>Second step 2 reads: 2. Copy the contents of the \Sources\Adprep folder...</p> <p>Should read: 2. Copy the contents of the \Support\Adprep folder...</p>	2/17/2012
516	"Installing a New Windows Server 2008 Child Domain" section, first paragraph	<p>Reads: If you have an existing domain, you can create a new child domain by creating a Windows Server 2008 R2 domain controller. Before you do, however, you must run Adprep /forestprep, as described in the "Installing the First Windows Server 2008 R2 Domain Controller in an Existing Forest or Domain" section.</p> <p>Should read: If you have an existing domain, you can create a new child domain by creating a Windows Server 2008 R2 domain controller. Before you do, however, if you have one or more Windows Server 2003 domain controllers in your forest, you must run adprep /forestprep, as described in the "Installing the First Windows Server 2008 R2 Domain Controller in an Existing Forest or Domain" section.</p>	2/17/2012
554	Practice 2	<p>Reads: ...installation DVD \Sources\Adprep folder.</p> <p>Should read: ...installation DVD \Support\Adprep folder.</p>	2/17/2012
566	Last sentence	<p>Reads: The underscore characters are a requirement of RFC 2052.</p> <p>Should read: The underscore characters are a requirement of RFC 2782.</p>	9/23/2011
575	Second paragraph, third sentence	<p>Reads: When you configure universal group membership caching on a domain controller in a branch office...</p> <p>Should read: When you configure universal group membership caching for a branch office site, a domain controller...</p>	2/17/2012

Page	Location	Description	Date corrected
575	Step 3	<p>Reads: The NTDS Site Settings Properties dialog box, shown in Figure 11-8, exposes the Enable Universal Group Membership Caching option You can select the check box and specify the GC from which to refresh the membership cache.</p> <p>Should read: The NTDS Site Settings Properties dialog box, shown in Figure 11-8, exposes the Enable Universal Group Membership Caching option. When you select the option, the default of the the Refresh Cache From option, <Default>, uses the most efficient route to a site with a global catalog server. It is recommended to use <Default>. Alternately, you can select a site from which to refresh the membership cache. Ensure that the site contains a working global catalog server.</p>	2/17/2012
595	First two bulleted items	<p>Should read: * Displaying replication status To display the status of inbound replication of a domain controller, type repadmin /showrepl DSA_LIST. * Displaying connection objects for a domain controller Type repadmin /showconn DSA_LIST to show the connection objects for a domain controller.</p>	2/17/2012
669	Fourth paragraph	<p>Reads: Note that to stop the AD DS service, the DC must be able to communicate with another DC that is running the service. If it cannot, you will not be able to stop the service. AD DS includes automatic checks and verifications that ensure that at least one DC is available at all times; otherwise, no one will be able to log on to the network.</p> <p>Should read: In Windows Server 2008 R2, you can stop the AD DS service if no other domain controller is present. However, if no other domain controller is present, you will not be able to log on to the DC that has the stopped AD DS service by using domain credentials should the session be closed or locked due to a screen saver. You will also not be able to use the local Domain Services Restore Mode (DSRM) password unless you previously modified the default HKLM\System\CurrentControlSet\Control\Lsa\DSRMAdminLogonBehavior Registry key settings. For more information on the restartable AD DS service, go to http://technet.microsoft.com/en-us/library/cc732714%28WS.10%29.aspx.</p>	9/23/2011
674	Steps 9 and 10	<p>The ends of steps 9 and 10 should be changed as follows.</p> <p>Reads: ...and then click the X button.</p> <p>Should read: ...and then click the Enter button.</p>	7/27/2012

Page	Location	Description	Date corrected
676	Steps 9 and 10	<p>The ends of steps 9 and 10 should be changed as follows.</p> <p>Reads: ...and then click the X button.</p> <p>Should read: ...and then click the Enter button.</p>	7/27/2012
679	Third bulleted item from bottom of page	<p>Reads: Backups cannot be performed to tape drives or dynamic volumes, only to network drives, removable hard drives configured as basic volumes, or DVDs and CDs.</p> <p>Should read: Backups can be performed to network drives, removable hard drives configured as basic volumes, DVDs and CDs, dynamic disks, and even virtual hard drives (VHD). For more information on Windows Server Backup for Windows Server 2008 R2, go to http://technet.microsoft.com/en-us/library/ee344835%28WS.10%29.aspx.</p>	9/23/2011
680	First bulleted item on page	<p>Reads: Backup operators cannot create scheduled backups; only members of the local Administrators group have this privilege in Windows Server 2008 R2. In most cases, this means being a member of the Domain Admins group on DCs.</p> <p>Should read: Backup operators can create scheduled backups in Windows Server 2008 R2.</p>	9/23/2011
692	Step 3, second paragraph, last line	<p>Reads: ...and, to do so, you must use the command line.</p> <p>Should read: ...and, to do so, you must use the command line or the graphical interface.</p>	11/18/2011
699	Exercise 1, step 6	<p>Reads: ...you created with Ntdusutil.exe.</p> <p>Should read: ...you created with Ntdsutil.exe.</p>	12/14/2012
701	Exercise 3, step 2	<p>Should read: ...and a C:\OriginalNTDS folder.</p>	7/27/2012
722	Exercise 1, step 6	<p>Reads: ...type the account name CONTOSO\Administrator...</p> <p>Should read: ...type the account name TreyResearch\Administrator...</p>	2/17/2012

Page	Location	Description	Date corrected
731	More Info reader aid, second paragraph, first sentence	<p>Reads: For information on creating a new forest and migrating its contents from one forest to another, look up Windows Server 2008 R2: The Complete Reference by Ruest and Ruest (McGraw-Hill Osborne, 2008 R2).</p> <p>Should read: For information on creating a new forest and migrating its contents from one forest to another, look up Windows Server 2008: The Complete Reference by Ruest and Ruest (McGraw-Hill Osborne, 2008).</p>	9/23/2011
742	After step 3	<p>The following Note reader aid should be added for information about using the DISM command.</p> <p>Should read: Note The DISM command Windows Server 2008 R2 administrators should get used to the DISM command, which is designed to replace OC Setup in future Server Core versions of Windows Server. For more information on DISM and additional installation and control options, go to http://technet.microsoft.com/en-us/library/dd744382%28WS.10%29.aspx.</p>	9/23/2011
747	Table 14-3, first row, Usage column	<p>Reads: ...register the Schmmgmt.dll first.</p> <p>Should read: ...register the Schmmgmt.dll first.</p>	2/17/2012
751	Last paragraph	<p>Paragraph should be a bulleted item.</p> <p>Reads: Any additional LDIF files you need for the instance...</p> <p>Should read: * Any additional LDIF files you need for the instance...</p>	9/23/2011
754	Step 2, code block	<p>Reads: cd windows\adam</p> <p>Should read: cd \windows\adam</p>	11/22/2013
761	Second bulleted item, code block	<p>Reads: Remove-ADUser -identity 'username' -server 'servername:port' -path 'distinguishedname of the path where the user is located'</p> <p>Should read: Remove-ADUser -identity 'username' -server 'servername:port' -partition 'distinguishedname of the instance partition'</p>	12/14/2012

Page	Location	Description	Date corrected
765	Step 10	<p>Reads: 10. Click OK to close the dialog box. In this case, you do not perform all activities. You only move SERVER04 to the new site link.</p> <p>Should read: 10. Click OK to close the dialog box. In this case, you do not perform all activities. You only move SERVER04 to the Servers container of the new site.</p>	7/27/2012
794	Step 11, last bulleted item	<p>Reads: The last option on the page provides further protection for the root CA. By selecting this option, you ensure that use of the CA will require administrative access and will work only with this level of access.</p> <p>Should read: The last option on the page provides further protection for the root CA. By selecting this option, you ensure that use of the CA will require administrative access and will work only with this level of access. In addition, using this option will allow administrators to work with third-party CPSs.</p>	11/18/2011
796	Exercise 2, step 1, second paragraph	<p>Reads: You need local administrative access rights only, but for the purposes of this exercise, the domain administrator account will also work.</p> <p>Should read: You need domain administrator access rights to perform this operation.</p>	7/27/2012
807	Step 8, first bulleted item, fourth sentence	<p>Reads: Also, use encryption to send the key to the CA.</p> <p>Should read: Also, use advanced Symmetric Algorithm to send the key to the CA.</p>	2/17/2012
810	Step 8	<p>Reads: 8. Click the computer name and then, in the Permissions section of the dialog box, select the Read, Enroll, and Autoenroll permissions in the Allow column.</p> <p>Should read: 8. Click the computer name and then, in the Permissions section of the dialog box, select the Read and Enroll permissions in the Allow column.</p>	2/17/2012
819	Exercise 1, step 8	<p>Should read: ...select the Read and Enroll permissions in the Allow column.</p>	7/27/2012

Page	Location	Description	Date corrected
903	First bulleted item, last sentence	<p>Reads: Because of this, all communications occur through port 433 over HTTPS.</p> <p>Should read: Because of this, all communications occur through port 443 over HTTPS.</p>	9/23/2011
922	Lesson 2, question 2 answers	<p>Reads: 2. Correct Answer: D A. Incorrect: AD CS is not supported on Server Core. B. Incorrect: AD FS is not supported on Server Core. C. Incorrect: AD RMS is not supported on Server Core. D. Correct: AD CS is not supported on Server Core, so you must reinstall the server with the full installation of Windows Server 2008 R2.</p> <p>Should read: 2. Correct Answer: D A. Incorrect: AD CS is not required on the same server as AD FS. B. Incorrect: AD FS is not supported on Server Core. C. Incorrect: AD RMS is not supported on Server Core. D. Correct: AD FS is not supported on Server Core, so you must reinstall the server with the full installation of Windows Server 2008 R2.</p>	9/23/2011

Page	Location	Description	Date corrected
927	Lesson 1, question 3 answers	<p>Reads:</p> <p>3. Correct Answers: C, D, E, and F</p> <p>A. Incorrect: Global groups cannot contain global groups from other domains.</p> <p>B. Incorrect: Global groups cannot contain global groups from other domains.</p> <p>C. Correct: Global groups can contain users in the same forest.</p> <p>D. Correct: Global groups can contain users in trusted domains.</p> <p>E. Correct: Global groups can contain users in the same domain.</p> <p>F. Correct: Global groups can contain global groups in the same domain.</p> <p>G. Incorrect: Global groups cannot contain domain local groups.</p> <p>H. Incorrect: Global groups cannot contain universal groups.</p> <p>Should read:</p> <p>3. Correct Answers: E and F</p> <p>A. Incorrect: Global groups cannot contain global groups from other domains.</p> <p>B. Incorrect: Global groups cannot contain global groups from other domains.</p> <p>C. Incorrect: Global groups can contain users in the same forest.</p> <p>D. Incorrect: Global groups can contain users in trusted domains.</p> <p>E. Correct: Global groups can contain users in the same domain.</p> <p>F. Correct: Global groups can contain global groups in the same domain.</p> <p>G. Incorrect: Global groups cannot contain domain local groups.</p> <p>H. Incorrect: Global groups cannot contain universal groups.</p>	9/23/2011
929	Lesson 3, question 3 answers	<p>Reads:</p> <p>3. Correct Answers: B, C, and D</p> <p>A. Incorrect: Account Operators does not have the right to shut down a domain controller.</p> <p>Should read:</p> <p>3. Correct Answers: A, B, C, and D</p> <p>A. Correct: Account Operators has the right to shut down a domain controller.</p>	9/23/2011
953	Lesson 1, question 3, answer C	<p>Reads:</p> <p>C. Correct: Windows Server 2008 forest functional level or higher is required for fine-grained password policies.</p> <p>Should read:</p> <p>C. Correct: Windows Server 2008 domain level or higher is required for fine-grained password policies. When you raise the forest functional level, you must also raise the domain functional level, making answer C the best answer.</p>	2/17/2012

Page	Location	Description	Date corrected
954	Lesson 2, question 2, answer C	<p>Reads: C. Correct: The /verify parameter verifies the health of an existing trust relationship. Some trusted users are able to access the resources, so the trust relationship is known to be healthy.</p> <p>Should read: C. Incorrect: The /verify parameter verifies the health of an existing trust relationship. Some trusted users are able to access the resources, so the trust relationship is known to be healthy.</p>	9/23/2011
957	Lesson 2, question 1 answers	<p>Reads: 1. Correct Answer: C</p> <p>Should read: 1. Correct Answer: D</p>	11/18/2011