

OFFICIAL MICROSOFT LEARNING PRODUCT

6436B

**Designing Windows Server® 2008 Active
Directory® Infrastructure and Services**

Companion Content

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

© 2012 Microsoft Corporation. All rights reserved.

Microsoft, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Product Number: 6436B

Released: 2/2012

MICROSOFT LICENSE TERMS

OFFICIAL MICROSOFT LEARNING PRODUCTS COURSEWARE – STUDENT EDITION – Pre-Release and Final Versions

These license terms are an agreement between Microsoft Corporation and you. Please read them. They apply to the licensed content named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this licensed content, unless other terms accompany those items. If so, those terms apply.

By using the licensed content, you accept these terms. If you do not accept them, do not use the licensed content.

If you comply with these license terms, you have the rights below.

1. OVERVIEW.

Licensed Content. The licensed content includes software, printed materials, academic materials (online and electronic), and associated media.

License Model. The licensed content is licensed on a per copy per device basis.

2. INSTALLATION AND USE RIGHTS.

- a. **Licensed Device.** The licensed device is the device on which you use the licensed content. You may install and use one copy of the licensed content on the licensed device.
- b. **Portable Device.** You may install another copy on a portable device for use by the single primary user of the licensed device.
- c. **Separation of Components.** The components of the licensed content are licensed as a single unit. You may not separate the components and install them on different devices.
- d. **Third Party Programs.** The licensed content may contain third party programs. These license terms will apply to your use of those third party programs, unless other terms accompany those programs.

3. PRE-RELEASE VERSIONS. If the licensed content is a pre-release ("beta") version, in addition to the other provisions in this agreement, then these terms also apply:

- a. **Pre-Release Licensed Content.** This licensed content is a pre-release version. It may not contain the same information and/or work the way a final version of the licensed content will. We may change it for the final, commercial version. We also may not release a commercial version. You will clearly and conspicuously inform any Students who participate in an Authorized Training Session and any Trainers who provide training in such Authorized Training Sessions of the foregoing; and, that you or Microsoft are under no obligation to provide them with any further content, including but not limited to the final released version of the Licensed Content for the Course.
- b. **Feedback.** If you agree to give feedback about the licensed content to Microsoft, you give to Microsoft, without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software, licensed content, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your feedback in them. These rights survive this agreement.
- c. **Confidential Information.** The licensed content, including any viewer, user interface, features and documentation that may be included with the licensed content, is confidential and proprietary to Microsoft and its suppliers.
 - i. **Use.** For five years after installation of the licensed content or its commercial release, whichever is first, you may not disclose confidential information to third parties. You may disclose confidential information only to your employees and consultants who need to know the information. You must have written agreements with them that protect the confidential information at least as much as this agreement.
 - ii. **Survival.** Your duty to protect confidential information survives this agreement.

iii. **Exclusions.** You may disclose confidential information in response to a judicial or governmental order. You must first give written notice to Microsoft to allow it to seek a protective order or otherwise protect the information. Confidential information does not include information that

- becomes publicly known through no wrongful act;
- you received from a third party who did not breach confidentiality obligations to Microsoft or its suppliers; or
- you developed independently.

d. **Term.** The term of this agreement for pre-release versions is (i) the date which Microsoft informs you is the end date for using the beta version, or (ii) the commercial release of the final release version of the licensed content, whichever is first ("beta term").

e. **Use.** You will cease using all copies of the beta version upon expiration or termination of the beta term, and will destroy all copies of same in the possession or under your control.

f. **Copies.** Microsoft will inform Authorized Learning Centers if they may make copies of the beta version (in either print and/or CD version) and distribute such copies to Students and/or Trainers. If Microsoft allows to such distribution, you will follow any additional terms that Microsoft provides to you for such copies and distribution.

4. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

a. **Media Elements and Templates.** You may use images, clip art, animations, sounds, music, shapes, video clips and templates provided with the licensed content solely for your personal training use. If you wish to use these media elements or templates for any other purpose, go to www.microsoft.com/permission to learn whether that use is allowed.

b. **Academic Materials.** If the licensed content contains academic materials (such as white papers, labs, tests, datasheets and FAQs), you may copy and use the academic materials. You may not make any modifications to the academic materials and you may not print any book (either electronic or print version) in its entirety. If you reproduce any academic materials, you agree that:

- The use of the academic materials will be only for your personal reference or training use
- You will not republish or post the academic materials on any network computer or broadcast in any media;
- You will include the academic material's original copyright notice, or a copyright notice to Microsoft's benefit in the format provided below:

Form of Notice:

© 2011 Reprinted for personal reference use only with permission by Microsoft Corporation. All rights reserved.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the US and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

c. **Distributable Code.** The licensed content may contain code that you are permitted to distribute in programs you develop if you comply with the terms below.

i. **Right to Use and Distribute.** The code and text files listed below are "Distributable Code."

- REDIST.TXT Files. You may copy and distribute the object code form of code listed in REDIST.TXT files.
- Sample Code. You may modify, copy, and distribute the source and object code form of code marked as "sample."
- Third Party Distribution. You may permit distributors of your programs to copy and distribute the Distributable Code as part of those programs.

ii. **Distribution Requirements.** For any Distributable Code you distribute, you must

- add significant primary functionality to it in your programs;
- require distributors and external end users to agree to terms that protect it at least as much as this agreement;
- display your valid copyright notice on your programs; and
- indemnify, defend, and hold harmless Microsoft from any claims, including attorneys' fees, related to the distribution or use of your programs.

iii. Distribution Restrictions. You may not

- alter any copyright, trademark or patent notice in the Distributable Code;
- use Microsoft's trademarks in your programs' names or in a way that suggests your programs come from or are endorsed by Microsoft;
- distribute Distributable Code to run on a platform other than the Windows platform;
- include Distributable Code in malicious, deceptive or unlawful programs; or
- modify or distribute the source code of any Distributable Code so that any part of it becomes subject to an Excluded License. An Excluded License is one that requires, as a condition of use, modification or distribution, that
 - the code be disclosed or distributed in source code form; or
 - others have the right to modify it.

- 5. INTERNET-BASED SERVICES.** Microsoft may provide Internet-based services with the licensed content. It may change or cancel them at any time. You may not use these services in any way that could harm them or impair anyone else's use of them. You may not use the services to try to gain unauthorized access to any service, data, account or network by any means.
- 6. SCOPE OF LICENSE.** The licensed content is licensed, not sold. This agreement only gives you some rights to use the licensed content. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the licensed content only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the licensed content that only allow you to use it in certain ways. You may not
- disclose the results of any benchmark tests of the licensed content to any third party without Microsoft's prior written approval;
 - work around any technical limitations in the licensed content;
 - reverse engineer, decompile or disassemble the licensed content, except and only to the extent that applicable law expressly permits, despite this limitation;
 - make more copies of the licensed content than specified in this agreement or allowed by applicable law, despite this limitation;
 - publish the licensed content for others to copy;
 - transfer the licensed content marked as 'beta' or 'pre-release' to any third party;
 - allow others to access or use the licensed content;
 - rent, lease or lend the licensed content; or
 - use the licensed content for commercial licensed content hosting services.
 - Rights to access the server software that may be included with the Licensed Content, including the Virtual Hard Disks does not give you any right to implement Microsoft patents or other Microsoft intellectual property in software or devices that may access the server.
- 7. BACKUP COPY.** You may make one backup copy of the licensed content. You may use it only to reinstall the licensed content.
- 8. TRANSFER TO ANOTHER DEVICE.** You may uninstall the licensed content and install it on another device for your personal training use. You may not do so to share this license between devices.
- 9. TRANSFER TO A THIRD PARTY.** You may not transfer those versions marked as 'beta' or 'pre-release' to a third party. For final versions, these terms apply: The first user of the licensed content may transfer it and this agreement directly to a third party. Before the transfer, that party must agree that this agreement applies to the transfer and use of the licensed content. The first user must uninstall the licensed content before transferring it separately from the device. The first user may not retain any copies.
- 10. EXPORT RESTRICTIONS.** The licensed content is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the licensed content. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.
- 11. NOT FOR RESALE SOFTWARE/LICENSED CONTENT.** You may not sell software or licensed content marked as "NFR" or "Not for Resale."

12. ACADEMIC EDITION. You must be a "Qualified Educational User" to use licensed content marked as "Academic Edition" or "AE." If you do not know whether you are a Qualified Educational User, visit www.microsoft.com/education or contact the Microsoft affiliate serving your country.

13. ENTIRE AGREEMENT. This agreement, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the licensed content and support services.

14. APPLICABLE LAW.

- a. **United States.** If you acquired the licensed content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.
- b. **Outside the United States.** If you acquired the licensed content in any other country, the laws of that country apply.

15. LEGAL EFFECT. This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the licensed content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.

16. DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS." YOU BEAR THE RISK OF USING IT. MICROSOFT GIVES NO EXPRESS WARRANTIES, GUARANTEES OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT EXCLUDES THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

17. LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. \$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.

This limitation applies to

- anything related to the licensed content, software, services, content (including code) on third party Internet sites, or third party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

Please note: As this licensed content is distributed in Quebec, Canada, some of the clauses in this agreement are provided below in French.

Remarque : Ce le contenu sous licence étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.

EXONÉRATION DE GARANTIE. Le contenu sous licence visé par une licence est offert « tel quel ». Toute utilisation de ce contenu sous licence est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection des consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 \$ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.

Cette limitation concerne:

- tout ce qui est relié au le contenu sous licence , aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers ; et
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Microsoft connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

Module 1

Overview of Active Directory® Design

Contents:

Lesson 3: Extending the Active Directory Design	8
Module Reviews and Takeaways	10
Lab Review Questions and Answers	11

Lesson 3

Extending the Active Directory Design

Contents:

Question and Answers

9

Question and Answers

Requirements for Extending Active Directory Functionality

Question: What other requirements have you seen that you cannot fulfill by using only AD DS?

Answer: Answers will vary. Most of the answers should be similar to the list above.

Module Reviews and Takeaways

Review questions

Question: Why is it important to identify business and security requirements before starting the Active Directory design?

Answer: It is important for the design to provide solutions for the requirements, and you cannot do this if you do not identify the requirements first.

Question: What is the most important question to answer when you are creating an AD DS design?

Answer: Answers may vary. In most cases, the most important question may be to decide how many forests you want to deploy within the organization, but students may come up with other answers, based on their experiences.

Question: What Active Directory technology or technologies can you use to secure a website that is exposed to Internet users?

Answer: You could use several of the Active Directory technologies. You could use AD CS to issue the certificates required to enable SSL for the site, or you could use AD LDS or AD FS to provide a directory service for the site.

Real-World Issues and Scenarios

Question: In most cases, you will not create a brand-new AD DS design for an organization. Instead, you will probably be upgrading the current Active Directory services or AD DS environment to Windows Server 2008 or Windows Server 2008 R2. What impact will this fact have on your AD DS design?

Answer: In most cases, the current environment sets limits on the potential AD DS design. For most companies, making significant changes to the current environment, such as changing the number of domains or forests, is too expensive and disruptive. Therefore, your design needs to account for these high-level components and work within them.

Lab Review Questions and Answers

Question: What are the core requirements that must be met in the Active Directory design at Contoso?

Answer:

- Design must support rapid company expansion to multiple new locations.
- Design must enable easy collaboration between users in multiple locations.
- Design must support secure external access by users to internal resources.
- Design must support the integration of A. Datum and Trey Research into the current Active Directory environment.
- Design should address issues, such as slow logon times and others, in the current environment.
- Design must provide a high level of security.
- Design must enhance the options for managing desktop computers.
- Design must limit administrative rights whenever possible.

Question: What are the potential constraints on the Active Directory design and deployment?

Answer: Design should minimize cost.

Module 2

Designing an AD DS Forest Infrastructure

Contents:

Lesson 1: Designing an AD DS Forest	2
Lesson 2: Designing AD DS Forest Trusts	5
Lesson 3: Planning for AD DS Schema Changes	7
Module Reviews and Takeaways	9
Lab Review Questions and Answers	10

Lesson 1

Designing an AD DS Forest

Contents:

Question and Answers	3
Additional Reading	4

Question and Answers

Design Models of AD DS Forests

Question: Which forest model do you use in your organization currently? Why?

Answer: Answers will vary. However, most students probably will answer that their organization uses either a single forest or an organizational forest model.

Additional Reading

Forest Functional Level Considerations

- [What are Active Directory Functional Levels?](#)

Lesson 2

Designing AD DS Forest Trusts

Contents:

Additional Reading

6

Additional Reading

What Is a Forest Trust?

- [Managing Forest Trusts](#)

Lesson 3

Planning for AD DS Schema Changes

Contents:

Question and Answers

8

Question and Answers

Schema Modification Options

Question: Has your organization ever made changes to its AD DS schema?

Answer: Answers may vary, but usually students will respond that changes to schema were made during Exchange Server implementation or when Active Directory was upgraded.

Module Reviews and Takeaways

Review questions

Question: What is the purpose of the Resource Forest Model?

Answer: You can use the Resource Forest Model in an environment with a particularly critical or secure application, shared folder, or other system resource. In such a scenario, administrators create a forest specifically for users who must access that resource.

Question: What must you set in AD DS to be able to establish a forest trust?

Answer: You must set the forest functional level to at least Windows Server 2003 so that you can establish a forest trust between two forests. Also, you must configure DNS in both forests, so that clients can resolve names from another forest.

Question: What is the most common reason that you might have for making updates to your schema?

Answer: You typically update your schema if you add a domain controller that runs on an older operating system, or if you deploy products such as Exchange Server or Lync Server into the existing environment.

Question: How is time used during the authentication process?

Answer: The timestamp helps prove that the authentication message was generated recently and is not a replay.

Lab Review Questions and Answers

Question: How would you apply the concepts discussed in this module to your own organization?

Answer: Answers will vary based on the students' organizations.

Module 3

Designing an AD DS Domain Infrastructure

Contents:

Lesson 1: Designing AD DS Domains	2
Lesson 2: Designing DNS Namespaces in an AD DS Environment	5
Module Reviews and Takeaways	8
Lab Review Questions and Answers	9

Lesson 1

Designing AD DS Domains

Contents:

Question and Answers	3
Additional Reading	4

Question and Answers

Design Models for AD DS Domains

Question: Which domain design model do you use in your environment? If you use multiple domains, why did you do so?

Answer: Answers may vary. However, most students probably will reply that they use the single domain model. Some also might use the regional model.

Considerations for Deploying Dedicated Forest Root Domains

Question: Are you using a forest root domain in your environment? Why or why not?

Answer: Answers may vary.

Additional Reading

Functional Levels for AD DS Domains

- [Understanding Active Directory Domain Services \(AD DS\) Functional Levels](#)

Lesson 2

Designing DNS Namespaces in an AD DS Environment

Contents:

Question and Answers	6
Additional Reading	7

Question and Answers

AD DS and DNS Integration

Question: How do you store your DNS zone data in your organization?

Answer: Answers may vary. However, most students will probably say that they are using Active Directory integrated zones.

Options for Designing an AD DS Namespace Strategy

Question: What kind of names are you using for your AD DS namespace?

Answer: Answers may vary.

Integrating the Public and Private DNS Namespaces

Question: Do you use split-DNS in your environment? Why or why not?

Answer: Answers will vary depending on the students' real environments.

Methods for Integrating Multiple DNS Namespaces

Question: What is the difference between a conditional forwarder and a stub zone?

Answer: The conditional forwarder provides a static mapping to DNS servers that can resolve queries for a specific namespace. However, a stub zone maintains a list of resource records for DNS servers in a specific zone. If DNS servers for a specific zone change, the stub zone updates automatically, while conditional forwarders require manual updating.

Additional Reading

AD DS and DNS Integration

- [How DNS Support for Active Directory Works](#)

Options for Designing an AD DS Namespace Strategy

- [How DNS Support for Active Directory Works](#)

Designing DNS Application Partitions

- [How DNS Support for Active Directory Works](#)
- DNS Help: Create a DNS application directory partition
- DNS Help: To enlist a DNS server in a DNS application directory partition

Module Reviews and Takeaways

Review questions

Question: Your organization has a Windows Server 2008 forest environment, but it has just acquired another organization with a Windows 2000 forest environment that contains a single domain. Users in both organizations must be able to access resources in each others' forests. What type of trust should you create between the forest root domains of each forest?

Answer: You will need to implement an external trust, because Windows 2000 does not support forest trusts. Only Windows Server 2003 or later supports forest trusts.

Question: If you want to integrate multiple internal namespaces, which technologies would you use?

Answer: Stub zones and delegation records.

Question: A user from Contoso attempts to access a shared folder in the Tailspin Toys domain and receives an Access Denied error. A trust relationship between these two domains exists. What must you do to provide the user with access?

Answer: First, you should check the direction of the trust and verify that selective authentication is applied. After that, you should check the ACL on shared folder.

Lab Review Questions and Answers

Question: How would you apply the concepts discussed in this module to your own organization?

Answer: Answers will vary based on the students' organizations.

Module 4

Designing AD DS Sites and Replication

Contents:

Lesson 1: Designing AD DS Sites	2
Lesson 2: Designing AD DS Replication	4
Module Reviews and Takeaways	7
Lab Review Questions and Answers	8

Lesson 1

Designing AD DS Sites

Contents:

Question and Answers

3

Question and Answers

Understanding AD DS Sites and Their Benefits

Question: Do you have sites deployed in your environment?

Answer: Answers will likely vary.

Collecting Information for an AD DS Site Design

Question: Why should you consider the number of users and computers in each location when you design AD DS sites?

Answer: You should consider the number of users and computers so you can determine whether to deploy a domain controller on-site and handle replication traffic over a WAN link, or whether to let users log on over a WAN link.

Lesson 2

Designing AD DS Replication

Contents:

Question and Answers	5
Additional Reading	6

Question and Answers

Understanding AD DS Replication

Question: Besides hosting the domain partition for its own domain, what else does a domain controller host?

Answer: Each domain controller in a forest also stores a copy of the Configuration Partition and the Schema Partition. However, changes in these partitions can be committed only on the appropriate holders of the operations master roles (also known as flexible single master operations, or FSMO, roles).

Components of Intrasite Replication

Question: Did you ever need to manually configure a connection object or the polling schedule?

Answer: Answers will vary.

Options for Designing Replication Topologies

Question: Which replication topology have you implemented in your environment?

Answer: Answers might vary; however, probably most students will reply that they have a full-mesh topology.

Choosing the Right Replication Protocol

Question: Do you have SMTP as a replication protocol in your environment? If yes, why can you not use RPC?

Answer: Most students will probably reply that they don't use SMTP. However, if someone is using it, the most probable reasons are an unreliable connection between sites or firewall rules.

Additional Reading

Planning to Replicate the Global Catalog, RODCs, and SYSVOL

- [SYSVOL Replication Migration Guide: FRS to DFS Replication](#)

Module Reviews and Takeaways

Review questions

Question: In a multi-site enterprise, why is it important that you identify all subnets and associate them with a site?

Answer: You can make the process of locating domain controllers and other services more efficient if you refer client computers to the correct site, based on the IP address for the client computer and the definition of subnets. If a client computer has an IP address that does not belong to a site, the client computer queries for all domain controllers in the domain, and that is not at all efficient. In fact, a single client computer can be performing actions against domain controllers in different sites, which (if those changes are not replicated yet) can lead to very strange results. It is important that each client computer knows what site it is in, and that is achieved by ensuring that domain controllers can identify which site a client computer is in.

Question: What is the purpose of a bridgehead server?

Answer: The bridgehead server is responsible for all replication into and out of the site for a partition. Instead of replicating all domain controllers in one site with all domain controllers in another site, bridgehead servers handle intersite replication.

Question: Which protocol can you use as an alternative to AD DS replication? What is the disadvantage of using it?

Answer: You can use SMTP, but it cannot replicate a domain partition.

Lab Review Questions and Answers

Question: How can you apply the concepts in this module to your own organization?

Answer: Answers will vary based on the students' organizations.

Module 5

Designing AD DS Domain Controllers

Contents:

Lesson 1: Designing Domain Controllers and Domain Controller Placement	2
Module Reviews and Takeaways	5
Lab Review Questions and Answers	6

Lesson 1

Designing Domain Controllers and Domain Controller Placement

Contents:

Question and Answers	3
Additional Reading	4

Question and Answers

Considerations for Deploying Domain Controllers on the Server Core

Question: What is the biggest benefit of running a domain controller on a server core?

Answer: The most important benefits are increased security and isolation.

Considerations for Planning Global Catalog Server Locations

Question: What is an alternative to using the global catalog when it comes to user authentication?

Answer: You can deploy Universal Group Membership caching.

Considerations for Planning Operations Master Server Locations

Question: How did you place operations master roles in your environment?

Answer: Answers may vary, but you can start discussion with this question.

Guidelines for Monitoring AD DS Domain Controllers

Question: Which tools do you use to monitor AD DS?

Answer: Answers may vary, but students will probably respond that they use Event Viewer, Microsoft System Center Operations Manager, or Performance Monitor.

Additional Reading

Planning Hardware Requirements for Domain Controllers

- [Assess Hardware Requirements](#)

Module Reviews and Takeaways

Review questions

Question: How can you prepare an unattended file easily for installation on a domain controller?

Answer: You can run the dcpromo.exe utility on a full version of Windows Server 2008 or Windows Server 2008 R2, and then export the configured settings when you reach the end of the wizard.

Question: What are the advantages and disadvantages of prepopulating the credentials for all users and computers in a branch office to that branch's RODC?

Answer: By prepopulating the credentials of users and computers in the branch RODC cache, you ensure that authentication performance is maximized on the first logon—after that, the credential would have been cached because the users are on the Allow list anyhow. Additionally, you ensure that if the WAN link is unavailable on the first logon, users can authenticate. The disadvantage is that, if there is a breach of physical security on the RODC, those credentials are exposed even if the users have not yet logged on in the branch.

Question: What kind of restore can you perform with AD DS?

Answer: You can perform authoritative restores, nonauthoritative restores, and restores of single objects within the Active Directory Recycle Bin.

Lab Review Questions and Answers

Question: How would you apply the concepts discussed in this module to your own organization?

Answer: Answers will vary based on the students' organizations.

Module 6

Designing AD DS Domain Administration

Contents:

Lesson 1: Planning the Delegation of AD DS Administration	2
Lesson 2: Designing the Structure of OUs	4
Lesson 3: Designing an AD DS Group Strategy	6
Lesson 4: Planning to Manage User and Computer Accounts	8
Module Reviews and Takeaways	10
Lab Review Questions and Answers	11

Lesson 1

Planning the Delegation of AD DS Administration

Contents:

Question and Answers

3

Question and Answers

IT Administrative Models

Question: What other organizational requirements might influence the administrative model that an organization chooses?

Answer: The organization might be anticipating change to its business structure, such as a reorganization or amalgamation. In this case, an administrative model based on the current business structure might not be suitable. Similarly, if an organization uses different business models in different parts of the organization, the IT administrative model might need to eschew alignment with business models and instead be based on a structure that is common to all parts of the organization.

Lesson 2

Designing the Structure of OUs

Contents:

Question and Answers

5

Question and Answers

Strategies for Designing OU Structures

Question: What OU design strategy do you use in your environment? Is that strategy the best fit for your organization?

Answer: Students will answer according to their environment, although some might not immediately recognize which strategy is being used. In these cases, it might be useful to draw the strategy on a whiteboard in order to identify unusual or hybrid strategies. Ideally, the OU design strategy should align as closely as possible with the organization's business practices.

Lesson 3

Designing an AD DS Group Strategy

Contents:

Question and Answers

7

Question and Answers

Guidelines for Developing a Group-Naming Strategy

Question: What naming conventions does your organization use? Have you used naming conventions in the past that worked well? Have you used any group naming conventions that didn't work well?

Answer: This is intended as a discussion starter to provide examples of naming conventions and why they might or might not be effective. If the students offer no examples, provide one from your experiences.

Lesson 4

Planning to Manage User and Computer Accounts

Contents:

Additional Reading

9

Additional Reading

Designing a User-Account Strategy

- [Redirecting the users and computers containers in Active Directory domains](#)

Implementing the Active Directory Recycle Bin

- [Active Directory Recycle Bin Step-by-Step Guide](#)

Tools for Automating User and Computer Account Management

- [Setting a User's Profile Attributes](#)
- [Modifying an Attribute for Several Users at Once](#)

Module Reviews and Takeaways

Review questions

Question: Which AD DS structures are most critical to administrative delegation, and why?

Answer: Organizational units, because they are the main objects that facilitate delegation and that enable the grouping of objects that have similar administration requirements.

Question: Which group-management method allows for more secure and efficient administration of AD DS groups?

Answer: Group nesting.

Question: Why should you always observe the principle of least privilege when assigning permissions for AD DS objects?

Answer: The principle of least privilege helps ensure that users do not have more access than they require. This helps ensure that your AD DS structure is not unnecessarily exposed to security risks. It also encourages the use of role-based access groups, and it improves awareness of which rights are assigned for objects in your AD DS environment.

Lab Review Questions and Answers

Question: How can you apply the principles and methods that this module covers to your own environment?

Answer: Answers will vary based on the students' organizations.

Module 7

Designing AD DS Group Policy

Contents:

Module Reviews and Takeaways	2
Lab Review Questions and Answers	3

Module Reviews and Takeaways

Review questions

Question: When designing a Group Policy infrastructure, what AD DS components play a critical part in determining your design?

Answer: Organizational units and security groups both play an important part in the design. The OU structure determines how effectively you can make use of inheritance, and how complicated the application of your GPOs needs to be. Security groups provide an additional level of GPO application via security group filtering.

Question: Why would you use Group Policy preferences to configure an aspect of the operating-system environment that you could configure by using Group Policy settings?

Answer: You might use Group Policy preferences when you do not want to enforce a setting but merely want to apply it across the organization and let users modify the behavior as needed.

Question: Why is inheritance important for the performance of Group Policy refresh?

Answer: GPOs within the same scope or on the same OU branch need to be processed if another GPO in the scope is modified.

Question: What is the most granular level at which you can apply a Group Policy preference setting?

Answer: You can apply Group Policy preferences to almost any one object using the advanced configuration parameters, although the most granular level for a GPO containing Group Policy preferences is still the OU.

Lab Review Questions and Answers

Question: How would you apply the principles and methods that this module covers in your own environment?

Answer: Answers will vary based on the students' organizations.

Module 8

Designing AD DS Security

Contents:

Lesson 1: Preparing to Design AD DS Security	2
Module Reviews and Takeaways	4
Lab Review Questions and Answers	5

Lesson 1

Preparing to Design AD DS Security

Contents:

Question and Answers

3

Question and Answers

Constraints to Designing AD DS Security

Question: What constraints have you seen in your organization that might prevent you from implementing a security policy? How have you addressed these constraints?

Answer: Answers will vary. The solutions to these types of constraints are often user education and increasing security incrementally.

Module Reviews and Takeaways

Review questions

Question: What constraints can applications put on your AD DS security design?

Answer: Some applications do not support long or complex passwords. This means that users must memorize multiple passwords if you require complex passwords.

Question: You decide to use the Security Configuration Wizard to configure the Windows Firewall settings for a domain controller. How can you apply the policy that you create to all domain controllers?

Answer: You can use the **Scwcmd** command-line tool to transform the policy into a GPO and to link the GPO to the Domain Controllers OU.

Question: What is the difference between *administrative autonomy* and *administrative isolation*?

Answer: *Administrative autonomy* means that you have complete administrative control over an AD DS component but that other administrators also have some administrative control over that component. *Administrative isolation* means that you have exclusive control over the AD DS component.

Real-World Issues and Scenarios

Question: Your organization has implemented a password policy that requires all users to use complex passwords that are at least 10 characters long. Some users with very limited permissions complain that this password is difficult for them to remember, and the security group has approved a simpler password for these users. How can you implement this without decreasing the password settings for other users?

Answer: You can implement a fine-grained password policy that applies to the users who have lower security requirements.

Question: Your organization has multiple domains in a single forest. Your security group has defined a requirement that only members of the Domain Admins group in the forest root domain should be able to change the membership list for the Domain Admins groups in the child domains. How can you implement this?

Answer: By default, only members of the Domain Admins group in each domain can modify the membership list for that group. To enforce the policy, add the members of the Domain Admins group in the forest root domain to a universal security group. Add this universal security group to the Domain Admins group in each child domain.

Lab Review Questions and Answers

Question: How can you apply the concepts in this module to your own organization?

Answer: Answers will vary based on the students' organizations.

Module 9

Designing a Public Key Infrastructure

Contents:

Lesson 1: Overview of PKI and AD CS	2
Lesson 2: Designing a Certification Authority Deployment	4
Lesson 3: Designing Certificate Templates	6
Lesson 4: Designing Certificate Distribution and Revocation	7
Module Reviews and Takeaways	12
Lab Review Questions and Answers	13

Lesson 1

Overview of PKI and AD CS

Contents:

Question and Answers

3

Question and Answers

Overview of the Certification Authority

Question: Why does the root CA typically issue certificates only to subordinate CAs?

Answer: For security reasons, the root CA is usually deployed as an offline CA. Because it protects the organizational PKI, we recommend that it remain offline. However, you must have another CA that can issue certificates.

What Is New for AD CS in Windows Server 2008?

Question: Which AD CS enhancement will benefit your organization the most?

Answer: Answers may vary, however, most students will probably choose OCSP, the restricted enrollment agent, and the new Group Policy settings.

Lesson 2

Designing a Certification Authority Deployment

Contents:

Question and Answers

5

Question and Answers

Building a CA Hierarchy

Question: What ties a subordinate CA to a root CA?

Answer: A trust, which is created when the subordinate CA receives its CA certificate from the root CA.

Usage Scenarios for CA Hierarchies

Question: Your organization would like to segment certificate distribution to vendors from the rest of your certificate distribution infrastructure. What type of CA would help facilitate this?

Answer: A subordinate CA.

Considerations for Deploying a Root CA

Question: What are the benefits of running AD CS on Windows Server 2008 R2 compared to Windows Server 2008?

Answer: Benefits include support for certificate enrollment across forests, database size reduction for high-volume CAs, and autoenrollment by using HTTP. Additionally, you can use the Standard version and still manage certificate templates.

Lesson 3

Designing Certificate Templates

Contents:

Question and Answers	7
Additional Reading	8

Question and Answers

Certificate Template Versions

Question: What should you do when you want to modify a version 1 certificate template?

Answer: You should first duplicate the version 1 template, and then upgrade the copy to either version 2 or version 3.

Methods for Modifying Certificate Templates

Question: What is the difference between modifying an original certificate template and superseding an existing certificate template?

Answer: Modifying a template affects only certificates issued thereafter while superseding an existing template affects both new and previously issued certificates.

Considerations for Designing Certificate Template Security

Question: Besides Read and Autoenroll, what other permission is required for the autoenrollment process?

Answer: Enroll is also required.

Additional Reading

Certificate Template Versions

- [Certificate Template Versions](#)

Lesson 4

Designing Certificate Distribution and Revocation

Contents:

Question and Answers	10
Additional Reading	11

Question and Answers

Certificate Distribution and Enrollment Options

Question: Which enrollment method is the most common when purchasing certificates from a trusted third-party certificate provider?

Answer: Manual enrollment and web enrollment are the most common methods used by third-party certificate providers.

Considerations for Designing Certificate Revocation

Question: Is using CRLs more beneficial than using online revocation checking?

Answer: It depends on the situation. In general, they are not. Checking a single certificate against a CRL is considered inefficient. However, checking thousands of certificates against a CRL is considered more efficient than an online check, such as for a smart card logon.

Considerations for Managing Key Archival and Recovery

Question: Why is it important to keep key recovery agent certificates secure?

Answer: You should keep key recovery agent certificates in a secure place because these certificates can be used to retrieve private keys for any archived certificate.

Additional Reading

Certificate Distribution and Enrollment Options

- [Selecting a Certificate Enrollment and Renewal Method](#)

Module Reviews and Takeaways

Review questions

Question: Why would an organization use PKI?

Answer: An organization would use PKI for certificate authentication, secure email, encryption on client computers, and smart card deployment. Some products, such as System Center Configuration Manager (SCCM) 2007 require PKI for full functionality.

Question: What is the difference between a public key and a private key in a PKI?

Answer: A public key encrypts data and is meant to be shared with others while a private key decrypts data and is not meant to be shared.

Question: What are some of the advantages of using a version 3 certificate template?

Answer: The version 3 certificate template supports new features available in a Windows Server 2008-based CA, such as CNG, which introduces support for Suite B cryptographic algorithms.

Question: Why would an organization use an enterprise root CA?

Answer: If an organization wants to use only one CA, and wants to use certificate templates and autoenrollment, then the only option is to use an Enterprise root CA.

Question: Why would you use manual certificate enrollment?

Answer: You would use manual enrollment if you want to specify additional options when enrolling for a certificate.

Lab Review Questions and Answers

Question: How would you apply the concepts discussed in this module to your own organization?

Answer: Answers will vary based on the students' organizations.

Module 10

Designing and Deploying AD RMS

Contents:

Lesson 1: AD RMS Overview	2
Lesson 2: Designing an AD RMS Deployment	4
Lesson 3: Extending the AD RMS Deployment Outside an Organization	6
Module Reviews and Takeaways	8
Lab Review Questions and Answers	9

Lesson 1

AD RMS Overview

Contents:

Question and Answers

3

Question and Answers

Usage Scenarios for AD RMS

Question: Are you already using an alternative technology to achieve these scenarios?

Answer: Answers will vary, but students might provide examples of how they are using some third-party solutions to achieve the same purpose.

AD RMS Deployment Scenarios

Question: Have you already implemented AD RMS in your environment? If yes, which deployment scenario are you using?

Answer: Answers will vary.

Lesson 2

Designing an AD RMS Deployment

Contents:

Question and Answers

5

Question and Answers

What Are AD RMS Rights and Rights-Policy Templates?

Question: Can an organization use AD RMS without using rights-policy templates? If they can, what limitations exist in that situation?

Answer: An organization can use AD RMS without using rights-policy templates. The main limitation is that users must manually set the authorized users and use rights each time they protect content with AD RMS.

Lesson 3

Extending the AD RMS Deployment Outside an Organization

Contents:

Question and Answers

7

Question and Answers

Options for Enabling External Users to Access AD RMS

Question: In which scenarios do you need to provide external access to AD RMS?

Answer: You need to provide external access to AD RMS if you want to distribute or accept AD RMS-protected documents from other organizations or if you want to send AD RMS-protected content over the Internet.

Module Reviews and Takeaways

Review questions

Question: What are some reasons to deploy AD RMS?

Answer: You can persistently protect sensitive information, you can let users communicate securely through email, and you can automatically protect document libraries in SharePoint.

Question: If you want to use a protected document from outside your organization, what should you configure?

Answer: You must configure a trust policy.

Question: What is the advantage of using Windows Live ID to share AD RMS-protected documents?

Answer: With Windows Live ID, a person who consumes a document does not need to have AD RMS deployed, so you can send an AD RMS-protected document to anyone who has Windows Live ID.

Lab Review Questions and Answers

Question: How can you apply the concepts discussed in this module to your own organization?

Answer: Answers will vary based on the students' organizations.

Module 11

Designing an AD LDS Infrastructure

Contents:

Lesson 1: AD LDS Deployment Scenarios	2
Lesson 2: Designing an AD LDS Server Deployment	4
Lesson 3: Designing AD LDS Replication	6
Module Reviews and Takeaways	8
Lab Review Questions and Answers	9

Lesson 1

AD LDS Deployment Scenarios

Contents:

Additional Reading

3

Additional Reading

Business Requirements That an AD LDS Deployment Provides

- [Active Directory Lightweight Directory Services Overview](#)

Considerations for Deploying LDAP-Compliant Application Directories

- [Active Directory LDAP Compliance](#)

Lesson 2

Designing an AD LDS Server Deployment

Contents:

Additional Reading

5

Additional Reading

Overview of AD LDS Components

- [Active Directory Lightweight Directory Services Getting Started Step-by-Step Guide](#)
- [Active Directory Lightweight Directory Services](#)

Lesson 3

Designing AD LDS Replication

Contents:

Additional Reading

7

Additional Reading

Overview of AD LDS Replication

- [Administering AD LDS Replication, Sites, and Configuration Sets](#)

Module Reviews and Takeaways

Review questions

Question: What are your options for high availability for AD LDS?

Answer: Load balancing is one option and adding additional replicas is another option.

Question: Do the instances that are part of the same configuration set run on the same or separate computers?

Answer: Instances that are part of the same configuration set can run on the same or separate computers.

Question: What information do you require to create an AD LDS replica?

Answer: You have to know the DNS name of the server that is running an AD LDS instance that belongs to the configuration set, as well as the LDAP port that was specified when the instance was created. You can also supply the distinguished names (DNs) of specific application directory partitions that you want to copy from the configuration set to the AD LDS instance that you are creating.

Question: True or false: You can deploy AD LDS on a computer currently configured as an AD DS domain controller.

Answer: True, although you must choose an appropriate TCP port on which the AD LDS service can listen for client requests because the default port conflicts with the AD DS port.

Real-World Issues and Scenarios

Question: Fabrikam has a development team working at two locations. The development team is working on the same directory-aware application. Currently, AD LDS is deployed at one location. Because of bandwidth constraints, the development team at the other location has reported poor performance when working with the application. What can you do to improve the performance?

Answer: Create a replica in the other site.

Question: The IT team at Contoso, Ltd., deployed AD LDS for their development team. To keep things simpler at that time, the team deployed AD LDS on an existing domain controller. The development team has asked for administrative access to perform tasks such as installing SSL certificates, stopping and starting services, and managing the AD LDS database. How should you proceed?

Answer: Move AD LDS to a member server and delegate management.

Lab Review Questions and Answers

Question: How can you apply the concepts in this module to your own organization?

Answer: Answers will vary based on the students' organizations.

Module 12

Designing an AD FS Infrastructure

Contents:

Lesson 1: Overview of an AD FS Design	2
Lesson 2: Designing an AD FS Deployment	5
Lesson 3: Designing AD FS Claims and Applications	8
Module Reviews and Takeaways	10
Lab Review Questions and Answers	11

Lesson 1

Overview of an AD FS Design

Contents:

Questions and Answers	3
Additional Reading	4

Question and Answers

Overview of AD FS Components and Concepts

Question: What are the differences between a Windows forest trust and an AD FS federation trust? What are the similarities?

Answer: A Windows forest trust requires connectivity between domain controllers in the two forests, while a federation trust has no connectivity between the federation servers. A federation trust does allow an FS-R to accept as valid authentications from an FS-A, similar to a forest trust.

Federated Web SSO with Forest Trust

Question: If your internal Active Directory environment consists of multiple forests in an account-and-resource forest scenario, which AD FS deployment scenarios should you consider?

Answer: You should consider the Federated Web SSO and the Federated Web SSO with Forest Trust scenarios.

Additional Reading

What Is AD FS?

- [Introducing AD FS 2.0](#)

Federated Web SSO with Forest Trust

- [AD FS Design Guide](#)

Options for Implementing AD FS User Account Stores

- [Understanding Account Stores \(for AD FS 1.x\)](#)
- [The Role of Attribute Stores \(for AD FS 2.0\)](#)

Lesson 2

Designing an AD FS Deployment

Contents:

Questions and Answers	6
Additional Reading	7

Question and Answers

Federated Applications

Question: If you are using the Federated Web SSO scenario, how can you obtain PKI certificates to minimize issues with AD FS and client configuration?

Answer: Obtain PKI certificates from a publicly trusted certification authority to ensure that the clients trust the certificates and that all of the AD FS components can access the certification authority's certificate revocation lists (CRLs).

Designing Components for the Account and Resource Partners

Question: If your organization has multiple Active Directory forests with trusts, are these trusts one-way or two-way? In a Federated Web SSO design, are there scenarios where an organization can be both an account partner and a resource partner?

Answer: Answers will vary.

Deploying and Securing AD FS Servers

Question: Does your organization publish the Microsoft Exchange Server 2007 Outlook® Web Access email client or Exchange Server 2010 Outlook Web App to the Internet? Can you use the same solution to publish AD FS?

Answer: Answers will vary.

Additional Reading

Choosing an AD FS Deployment Scenario

- [Identifying Your AD FS Deployment Goals](#)

Public Key Infrastructure Certificates

- [ADFS Certificates - SSL, Token Signing, and Client Authentication Certs](#)

Implementing a Web SSO Design

- [Overview of Active Directory Federation Services](#)

Designing Components for the Account and Resource Partners

- [ADFS Design and Deployment Guide](#)

Lesson 3

Designing AD FS Claims and Applications

Contents:

Additional Reading

9

Additional Reading

Options for Configuring AD FS Claims

- [Understanding Claims](#)

Using Claims-Aware and Token-Based Applications

- [Understanding Application Types for AD FS Federation](#)

Module Reviews and Takeaways

Review questions

Question: What are the three AD FS deployment scenarios?

Answer: Web SSO, Federated Web SSO, and Federated Web SSO with Forest Trust.

Question: What is the primary reason to deploy the Federated Web SSO with Forest Trust scenario?

Answer: To support Windows token-based applications without the need for “shadow” accounts.

Question: What is the primary restriction to using the Kerberos protocol to sign tokens in your AD FS deployment?

Answer: The FS-R and the web-application server must be in the same Active Directory forest.

Lab Review Questions and Answers

Question: How can you apply the principles and methods covered in this module to your own environment?

Answer: Answers will vary based on the students' organizations.

Module 13

Designing AD DS Transitions

Contents:

Lesson 2: Designing a Domain Upgrade Strategy	2
Lesson 3: Designing a Domain Restructure Strategy	4
Lesson 4: Designing AD DS Domain Renaming	6
Module Reviews and Takeaways	8
Lab Review Questions and Answers	9

Lesson 2

Designing a Domain Upgrade Strategy

Contents:

Additional Reading

3

Additional Reading

Options for Implementing a Domain Upgrade Strategy

- [Guide for Upgrading to Windows Server 2008](#)
- [Installing Windows Server 2008 R2](#)

Documenting the Current Environment

- [Microsoft Active Directory Topology Diagrammer](#)

Lesson 3

Designing a Domain Restructure Strategy

Contents:

Additional Reading

5

Additional Reading

Using ADMT for Domain Restructuring

- [ADMT Guide: Migrating and Restructuring Active Directory Domains](#)

Lesson 4

Designing AD DS Domain Renaming

Contents:

Additional Reading

7

Additional Reading

Overview of the Domain-Renaming Process

- [Administering Active Directory Domain Rename](#)
- [Microsoft Exchange Domain Rename Fixup Tool](#)

Considerations for Renaming Domains

Module Reviews and Takeaways

Review questions

Question: You are upgrading a Windows Server 2003 domain to Windows Server 2008 R2. Which transition strategy is typical if you are allocating new, replacement hardware for the domain controllers in your domain?

Answer: The replacement upgrade is strategy you would most likely use. Install Windows Server 2008 R2 as new domain controllers in the existing domain. When you have at least two Windows Server 2008 R2 domain controllers joined to the domain, you can decommission the existing Windows Server 2003 domain controllers, and then change the forest and domain functional levels accordingly.

Question: You need to upgrade a domain containing four domain controllers that run the Windows Server 2003 R2 Standard 86-bit version to Windows Server 2008 R2. Can you do an in-place upgrade on the four domain controllers? Why or why not?

Answer: No. You cannot upgrade these domain controllers by using an in-place upgrade because Windows Server 2008 R2 does not support 86-bit-based hardware.

Question: To preserve group membership, which AD DS object do you move first during the interforest ADMT migration process: user accounts or global groups?

Answer: Move global groups first, and then move the user accounts.

Lab Review Questions and Answers

Question: How would you apply the principles and methods covered in this module in your own environment?

Answer: Answers will vary based on the students' organizations.