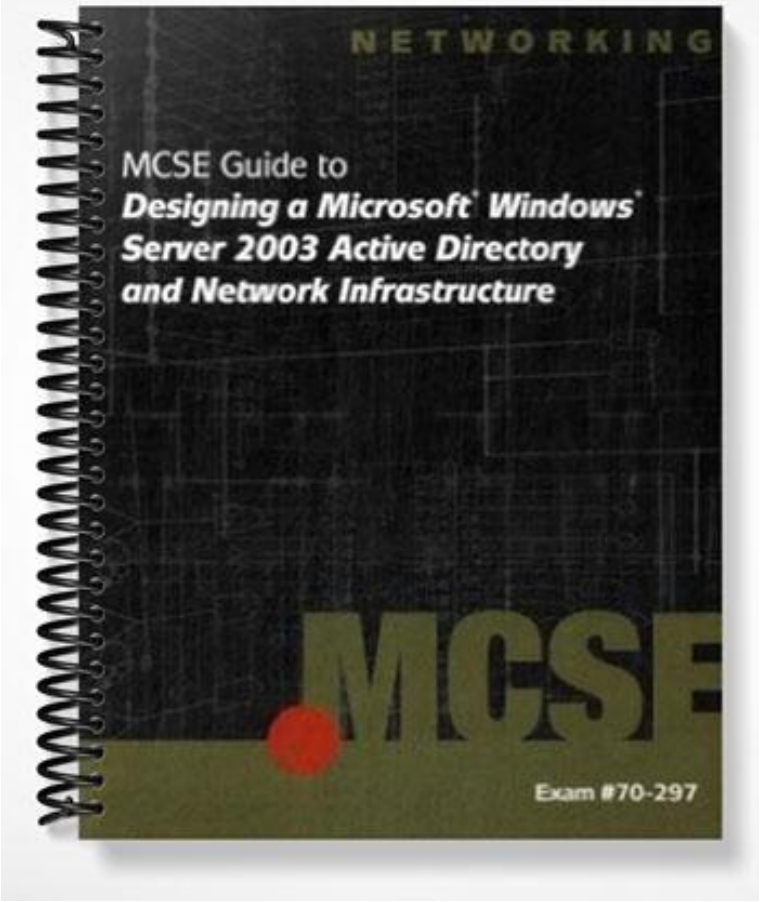
SOLUTIONS MANUAL



Chapter 2: Developing the Active Directory Infrastructure Design

Objectives

After reading the chapter and completing the exercises, students should be able to:

1.5 Design the Active Directory infrastructure to meet business and technical requirements.
- 1.5.1 Design the envisioned administration model.
- 1.5.2 Create the conceptual design of the Active Directory forest structure.
- 1.5.3 Create the conceptual design of the Active Directory domain structure.
- 1.5.5 Create the conceptual design of the organizational unit (OU) structure.
- 1.5.4 Design the Active Directory replication strategy.

Teaching Tips

Introduction

1. Ask students to identify the data that an organization will need in order for it to start designing Active Directory. Note that during the initial stages of an Active Directory services infrastructure design phase, one should identify the administrative model that will be implemented.

Assessing and Designing the Administrative Model (Objective 1.5.1)

1. Introduce the topic by discussing the rationale behind Microsoft's decision to rethink Security boundaries, including whether the domains actually represent a boundary, or whether, in fact, the forest should be viewed as the secondary boundary.

2. Clearly identify the roles of the service administrator and the data administrator. Note that the concept of viewing the above roles as separate groups is new to Microsoft; therefore students should be conversant with the new concepts and ideas.

3. The terms autonomy and isolation are new to Microsoft literature. It is therefore essential that the terms be understood. Clearly define for following concepts: service autonomy, data autonomy, service isolation, and data isolation. Point out that in Active Directory, administrators can delegate both service administration and data administration in order to achieve either autonomy or isolation between organizations.

Quick Quiz

1. If an entity requires _____, then a degree of independence is required.
   Answer: autonomy

2. _____ implies that only the administrators of the resource have access and that there are no other administrators elsewhere with sufficient rights to access or manage those same resources.
   Answer: Isolation

3. True or False: The data administrator is responsible for a subset of objects in Active Directory and has no rights to any objects elsewhere in the forest.
   Answer: True

4. True or False: Service administrators are responsible for maintaining the Active Directory infrastructure and for ensuring that this infrastructure provides the necessary functions and services to end users.
   Answer: True

Assessing and Defining the Forest Design (Objective 1.5.2)

1. In this section, you should examine different forest designs, the scenarios for which they are relevant, and present a guideline that will enable students to determine which design best suits a particular organization. The following is a list of topics that will play into decisions made regarding forest design:

Forest Design:	▪ Organizational ▪ Operational ▪ Legal ▪ Naming considerations ▪ Timescales ▪ Management overhead ▪ Test environments ▪ External facing environments

2. It is important for students to understand that at this stage in the design phase, the ideal scenario is that of a single forest. This model will always offer the lowest administrative overhead and total cost of ownership and it is always prudent to attempt to design Active Directory as a single forest wherever possible.

3. The following tables provide a summary of the forest models:

Multiple Forests	
Advantages	**Disadvantages**
Separate schemas, allowing for forest autonomy at the schema level.	No simple sharing of network resources; collaboration between forests needed.
Separate configuration partitions, allowing for forest autonomy at the configuration level.	Requires an external trust(s) to domain(s) in other forest(s) in order to share resources.
No requirements for interbusiness trusts; each forest is isolated from every other forest. Separate forest service admins, allowing for business autonomy and isolation.	Global catalog (GC) queries can access objects only in the local forest. A number of disparate schemas might exist - consolidation of forests at a later date might prove difficult.
Mitigates known Active Directory vulnerabilities (because each is isolated from every other).	Requires some Meta-Directory to manage inter-forest synchronization and generation of a common global address book (if a common, global address book is required).
No dependency on any other business; each business has complete independence in its own forest.	Higher design and implementation costs.
Can completely and easily separate DNS hierarchies - each business can choose its own namespace and no interoperability is necessarily required between these namespaces.	
Allows for the segregation of externally facing Active Directory environments.	
Allows for the segregation of test Active Directory environments.	

Single Forest	
Advantages	**Disadvantages**
Single forest - allows for simple sharing of objects across domains.	Controlled change management plan required for forestwide operations, because of potential impact to all domains.
A single exchange organization can be deployed, using the same directory as Active Directory.	Control over Enterprise components required, which are shared across multiple domains
Single replicated GC and therefore, a common Global Address Book view in Exchange.	Thought, collaboration, and planning required to meet each domain's security needs.
Single set of object entities to manage, such as schema and configuration.	Thought and planning required to deliver horizontal Exchange system management vs. vertical divisional Active Directory management.
Lower design and implementation costs.	Does not cater to test environments. Does not cater to externally facing environments.

Teaching Tip:	The following Web site provides detailed information about mapping design requirements to forest design models. Pay particular attention to Table 2.1 which identifies the forest design model scenario that best meets your needs based on the autonomy, isolation, and connectivity factors identified: http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dssbc_logi_jybq.asp

4. Ownership and sponsorship are very important topics that traditionally have not been addressed in Microsoft literature. Introduce subjects such as ownership, accountability, and change management, and note that without these aspects the environment can quickly fall into chaos.

Assessing and Creating the Domain Design (Objective 1.5.3)

1. This section should be used to discuss the issues that affect the domain design within a forest. Note that all forests contain at least one domain, but the decision to deploy additional domains is influenced by geographic, network, and service autonomy factors.

Domain Design Factors:	▪ ***Geographic separation:*** Given that Active Directory data is replicated per partition, a geographic domain design can also be used to better control and manage replication across disparate regions. Furthermore, GCs in any one region would replicate only local domain data with DCs/GCs in the same region and would replicate only partial (around 50 percent) data from other regional domains. Such a regional design split can therefore be used to better control replication between the different regions within an enterprise. ▪ ***Network Limitations:*** In certain parts of the world, WAN links between small offices and the nearest hub site can prove costly to implement, costly to maintain, and are often unreliable. If this is the case within your organization, then the domain design might be influenced by these links. ▪ ***Service autonomy:*** If an organization is made up of independent businesses, these different entities, although keen to share a common infrastructure and realize the lower associated TCO, might require a degree of autonomy within their own domain. The best solution available is that the business deploys a separate domain within the forest.

2. Ask students to suggest factors that influence the names chosen within each forest. Point out that when deploying the first domain in a forest, the DNS name chosen is used as the suffix for all other domains in the same tree of the forest.

3. Discuss the reasons for deploying a dedicated root domain. Ask students to discuss the implications of the dedicated root domain being politically and geographically neutral. Caution students that even though a dedicated root domain stops domain admins in other domains from elevating their rights so they have EA or SA rights, it is still possible for malicious administrators to grant themselves forest service admin rights or indeed DA rights in any other domain, using specialized tools and procedures.

Dedicated Root Domain:	***Advantages:*** ▪ Forest service admins are separated from domain service admins: ▪ Simpler to reconfigure the forest: ▪ Politically neutral ***Disadvantage:*** ▪ Additional service administrator roles need to be managed, along with an additional DNS zone and additional DCs.

Regional Domains:	***Disadvantages of introducing additional domains:*** ▪ Multiple service admin groups ▪ Additional overhead in duplicating settings ▪ Interdomain object moves

4. Engage students in a discussion about the issues involved when deploying multiple domains. Suggest circumstances where the deployment of a single domain would be more appropriate.

5. Clearly outline the issues concerning the functional domain model. Note the additional requirement of general collaboration between domains.

Teaching Tip:	For more information about determining the number of domains, visit the following Web site: http://www.microsoft.com/resources/documentation/windowsserv/2003/all/deployguide/en-us/dssbc_logi_oyuo.asp

6. One question that should be posed to students is: "Should new domains be created as the root of a new tree, within an existing tree, or within the root tree?" The answers to these questions depend on the reasons used to deploy new domains and the nature of the organization. The following table provides a comparison of the different domain models.

Comparing Trees with Domains		
	Advantages	**Disadvantages**
Single Tree	Only one namespace needs to be created and managed	Disparate, autonomous businesses are constrained to using the first namespace
	No interoperability issues exist between disparate namespaces	Businesses do not have autonomy within their own namespace
Multiple Trees	Disparate businesses can use their own different namespaces	Multiple DNS names
	Autonomy within the business namespace	Increased DNS maintenance

Single Domain Forest	Reduced administrative overhead	The domain can never be renamed (without being rebuilt)
	Reduced hardware	Forest service admins cannot be separated from domain service admins
	Reduced design effort. All DCs can also be GCs, thus removing the need to design GC placement.	This domain will always own the forest service admins roles. This might not be appropriate politically if further domains join the forest. All objects are replicated to every DC in every region, which can result in unacceptable levels of replication traffic.

Quick Quiz

1. True or False: Each DNS namespace within the organization must be unique.
   Answer: True

2. True or False: An advantage of the multiple forest model is that it allows for simple sharing of objects across domains.
   Answer: False

3. The first domain deployed into any forest is known as the _____ domain.
   Answer: root

4. The _____ model implies that a separate domain is created for each distinct region within the organization.
   Answer: regional

Developing the OU Model (Objective 1.5.5)

1. OU design is generally dictated by three factors: the way in which the business is administered, the way in which group policy needs to be deployed, the need to hide sensitive objectives from users. Note that the OU structure within each domain can be designed in one of many different ways. It is therefore important to examine those factors that affect the design closely, so that the design options available can be narrowed down to a small subset of all available options.

2. The three most popularly used OU models are the functional, geographic, and object type models. A basic introduction to these concepts and their applicability is required.

OU Design Models:	▪ ***Geographic model:*** Starts by creating geography-based OUs at the root of the domain and then further segregating objects below that, as appropriate. ▪ ***Functional model:*** Starts by creating functional-based OUs at the root of the domain, and then further segregating objects below that as appropriate. ▪ ***Object Type Model:*** Starts by creating object type-based OUs at the root of the domain, and then further segregating objects below that as appropriate.

Developing the Replication Design (Objective 1.5.4)

1. The one remaining Active Directory infrastructure-related piece of the puzzle is that of replication design. Explain that without a replication design and topology, all the designs arrived at previously relating to forests and domains and OUs are moot.

2. Active Directory replication involves various terms, concepts, and objects that are used to create a replication topology. Consequently, the following topics should be clearly explained:

Active Directory Replication:	▪ ***Sites:*** Collections of well-connected IP subnets. ▪ ***Subnets:*** Logical collections of contiguous IP addresses, all within the same LAN segment or virtual segment. ▪ ***Site links:*** Links between sites that must be established to determine the direction and nature of flow of Active Directory data replication between sites. ▪ ***Site link bridges:*** Sites that do not share a common site link but do share common Active Directory data, such as an Application Directory partition, can be bridged using site link bridges. ▪ ***Connection objects:*** In order that Active Directory data can be replicated both within and between sites, connection objects are established between DCs. ▪ ***Multimaster replication:*** Application directory partitions are available only if the Domain Naming Master role is hosted by a Windows Server 2003 DC or above. Because changes can be made on any one of the DCs holding a read/write copy of the appropriate partition, replication is described as "multimaster," because no one server has the only changeable copy of any partition. ▪ ***Knowledge Consistency Checker (KCC):*** Evaluates, at regular intervals, the site topology and available DCs and then generates intra-site connection objects for the local DC with other DCs in the same site to ensure efficient replication of Active Directory data. ▪ ***Inter Site Topology Generator and bridgehead servers:*** Establishes all inter-site connection objects. ▪ ***SYSVOL:*** Typically used to house scripts and group policies. ▪ ***File Replication System (FRS):*** Used to replicate SYSVOL data between DCs in the same domain. ▪ ***Topology options:*** Includes ring, full mesh, hub and spoke, and a hybrid. ▪ ***Ownership:*** A topology owner has sole control and access to the replication topology within Active Directory.

Teaching Tip:	For information about creating a site link bridge design to control active directory replication flow, visit the following Web site: http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dssbd_topo_ugzv.asp

Quick Quiz

1. A(n) _____ is a collection of well-connected IP subnets.
   Answer: site

2. A(n) _____ is a logical collection of contiguous IP addresses, all within the same LAN segment or virtual segment.
   Answer: subnet

3. True or False: A 64Kb WAN link will have a higher cost associated with it than will a 1Mb link.
   Answer: True

4. A(n) _____ topology involves constructing a loop with each site connected to two neighbor sites.
   Answer: ring

Class Discussion Topics

1. Discuss the differences in the following roles: service administrator and data administrator.

2. Why is isolation and autonomy considered important concepts when designing forests?

3. Discuss the advantages of the various topology options.

Additional Projects

1. Describe the steps involved in creating an organizational unit.
2. Describe the steps involved in creating subnets in Windows Server Active Directory.

Solutions to Additional Projects

1. To create an organizational unit:
   a. Open Active Directory Users and Computers by clicking Start, Administrative Tools, Active Directory Users and Computers.
   b. Highlight the container, domain or parent organizational unit, in to which you want to create the new organizational unit.
   c. Click the Action menu and select New, then Organizational Unit.
   d. Type the name of the organizational unit in the Name text box, for example Member Servers.
   e. Click OK.

2. To create a subnet:
   a. Start the Active Directory Sites and Services Microsoft Management Console (MMC) snap-in.
   b. Double-click the Sites container.
   c. Right-click the Subnets container.
   d. Click New Subnet.
   e. In the Address field, type the Internet Protocol (IP) address and mask that you want to use.
   f. Select a site object for this subnet.
   g. Click OK.