TRUE/FALSE

1. For most applications, a single-domain, single-forest design will work.

   ANS: T PTS: 1 REF: 2

2. A domain functional level or forest functional level can be raised and then undone (or lowered) as necessary.

   ANS: F PTS: 1 REF: 9

3. If you want users or groups to be able to access a resource using SID history, you must enable SID filtering.

   ANS: F PTS: 1 REF: 29

4. SID filtering should be disabled by an automated process.

   ANS: F PTS: 1 REF: 29

5. It's possible to create alternative UPN suffixes and assign these to users in the domain.

   ANS: T PTS: 1 REF: 30

MULTIPLE CHOICE

1. An Active Directory domain is hosted on a server called a ____.
   a. member server
   b. domain master
   c. domain controller
   d. role master

   ANS: C PTS: 1 REF: 2

2. The ____ for Active Directory defines the objects that can be created in Active Directory.
   a. schema
   b. directory
   c. database
   d. template

   ANS: A PTS: 1 REF: 3

3. ____ is an Active Directory preparation tool that can modify the schema by adding objects and properties needed to support Windows Server 2008 domain controllers.
   a. ADSIEdit
   b. ADPrep
   c. DCPromo
   d. GPUpdate

   ANS: B PTS: 1 REF: 3

4. Trusts within a forest are ____ trusts.
   a. one-way
   b. foreign
   c. non-transitive
   d. transitive

   ANS: D PTS: 1 REF: 3

5. A ____ is a group of well-connected computers or well-connected subnets.
   a. domain
   b. site
   c. forest
   d. trust

   ANS: B PTS: 1 REF: 4

6. Fine-grained password policies can be implemented if the domain functional level is set to at least ____.
   a. Windows NT
   b. Windows Server 2000 Native
   c. Windows Server 2003
   d. Windows Server 2008

   ANS: D PTS: 1 REF: 9

7. Forest trusts are possible once the forest functional level has been raised to ____.
   a. Windows NT
   b. Windows Server 2000 Native
   c. Windows Server 2003
   d. Windows Server 2008

   ANS: C PTS: 1 REF: 9

8. Fine-grained password and account ____ policies are a significant addition to Windows Server 2008.
   a. lockout
   b. length
   c. timeout
   d. login

   ANS: A PTS: 1 REF: 10

9. When you see the forest functional level is Windows Server 2008, you also know that every domain and domain controller in the forest must be running at least ____.
   a. Windows NT
   b. Windows Server 2000 Native
   c. Windows Server 2003
   d. Windows Server 2008

   ANS: D PTS: 1 REF: 12

10. In a ____, users in each domain can be granted access to resources in both domains.
    a. one-way trust
    b. two-way trust
    c. foreign trust
    d. restricted trust

    ANS: B PTS: 1 REF: 16

11. A ____ trust creates an explicit trust relationship between two domains and is not transferred to any other domains.
    a. non-transitive
    b. transitive
    c. one-way
    d. foreign

    ANS: A PTS: 1 REF: 16

12. A ____ trust is granted between several domains without creating explicit trust relationships between the different domains.
    a. non-transitive
    b. one-way
    c. transitive
    d. foreign

    ANS: C PTS: 1 REF: 16-17

13. The ____ authentication option allows Windows to automatically authenticate any users in another forest to access resources in the local forest.
    a. domain-wide
    b. tree-wide
    c. schema-wide
    d. forest-wide

ANS: D PTS: 1 REF: 18

14. The ____ authentication option can be used to prevent users in another forest from automatically being authenticated.
    a. restricted
    b. selective
    c. filtered
    d. one-way

    ANS: B PTS: 1 REF: 18

15. When selective authentication is implemented on a forest trust, you need to grant the ____ permission on each server or computer where access is granted.
    a. Allowed to Authenticate
    b. Replace Token
    c. Run as Service
    d. Act as Part of the Operating System

    ANS: A PTS: 1 REF: 23

16. The ADPrep switch ____ is used to prepare the forest for Windows Server 2008 or Windows Server 2008 R2 domain controllers.
    a. `/ForestBuild`
    b. `/ForestNew`
    c. `/ForestPrep`
    d. `/ForestSelect`

    ANS: C PTS: 1 REF: 24

17. You can easily determine what servers hold all the roles by opening a command prompt and entering the following command: ____
    a. `netdom query trust`
    b. `netdom query fsmo`
    c. `netdom query pdc`
    d. `netdom query dc`

    ANS: B PTS: 1 REF: 25

18. ____ is used when objects are migrated between domains in separate forests.
    a. Interforest migration
    b. Intraforest migration
    c. Interdomain migration
    d. Intradomain migration

    ANS: A PTS: 1 REF: 27

19. Access to any resource within the domain is controlled by a(n) ____.
    a. Access Control Entity
    b. Discretionary Access Control Object
    c. Discretionary Access Control List
    d. Access Control List

    ANS: C PTS: 1 REF: 27

20. ____ prevents the risk of an attacker obtaining SID history data by blocking the use of any SIDs that did not originate in the same domain.
    a. SID blocking
    b. SID selecting
    c. SID masking
    d. SID filtering

    ANS: D PTS: 1 REF: 28

21. You can disable SID filtering using the ____ command on the trusting domain.
    a. `Netdom`
    b. `Netf`
    c. `Wscript`
    d. `Netsh`

    ANS: A PTS: 1 REF: 29

COMPLETION

1. An Active Directory _____ includes one or more trees comprised of one or more domains.

   ANS: forest

   PTS: 1 REF: 3

2. A(n) _____ is used within a domain to organize objects.

   ANS:
   Organizational Unit (OU)
   Organizational Unit
   OU

   PTS: 1 REF: 4

3. _____ is achieved when an organization can independently manage their data.

   ANS: Data autonomy

   PTS: 1 REF: 14

4. _____ is used when objects are migrated between domains in the same forest.

   ANS: Intraforest migration

   PTS: 1 REF: 27

5. ADMT v3.1 should be installed and run on a Windows Server 2008 domain controller in the _____ domain.

   ANS: target

   PTS: 1 REF: 32

MATCHING

Match each term with the correct statement below.

a. security identifier (SID)
b. isolation
c. Active Directory tree
d. Group Policy
e. ADMT
f. Active Directory domain
g. global catalog
h. autonomy
i. User Principal Name (UPN)

1. Is an administrative boundary and holds a database of objects
2. Includes one or more domains with a common namespace
3. Is a listing of all the objects in the entire forest
4. Is the tool used to automate the management and administration of users and computers in the domain
5. Provides independence, allowing a department or group to make decisions based on their own needs within the organization
6. Provides independent and exclusive control of a resource

7. Can be used to migrate objects from one domain to another within the same forest or between different forests
8. Is used to uniquely identify an object in a domain
9. Allows a user to log on with an account that looks like an e-mail address

1. ANS: F PTS: 1 REF: 2
2. ANS: C PTS: 1 REF: 2
3. ANS: G PTS: 1 REF: 3
4. ANS: D PTS: 1 REF: 4
5. ANS: H PTS: 1 REF: 14
6. ANS: B PTS: 1 REF: 14
7. ANS: E PTS: 1 REF: 26
8. ANS: A PTS: 1 REF: 27
9. ANS: I PTS: 1 REF: 30

SHORT ANSWER

1. You are designing a plan that will merge two companies and you need to create a forest trust relationship between two forests. What are some considerations you should keep in mind?

   ANS:
   When designing a plan that will merge two companies, you need to create a forest trust relationship between the two forests. Forest trusts are possible once the forest functional level has been raised to Windows Server 2003. You can only raise the forest functional level when all domains in the forest have reached the same level, and you can only raise the domain to a functional level when all the domain controllers are running the appropriate versions of Windows Server. Your design plans will need to include the following steps to support forest trusts:

   Verify that all domain controllers are running at least Windows Server 2003, and if not, include plans to upgrade them.

   Raise the domain functional levels of each domain in each forest to at least Windows Server 2003.

   Last, you'll need to raise the forest functional level of each forest to at least Windows Server 2003.

   PTS: 1 REF: 9

2. Discuss the difference between domain controllers and servers when raising the level to Windows Server 2008.

   ANS:
   One might mistakenly think that all servers must run Windows Server 2008 to raise the level to Windows Server 2008. This is not true. Only the domain controllers must meet the required level. You can run Windows Server 2000 member servers in a domain at the domain functional level of Windows Server 2008.

   PTS: 1 REF: 10

3. Explain the difference between autonomy and isolation.

   ANS:

When deciding on the number of forests and domains you need, you often need to identify the autonomy and isolation requirements. These requirements are determined by the business needs, but are implemented by creating one or more forests. When considering autonomy and isolation, note two important points:
• Autonomy provides independent, but not exclusive, control of a resource.
• Isolation provides independent and exclusive control of a resource.

PTS: 1 REF: 13

4. Beyond autonomy, what are two other reasons to create separate domains?

ANS:
To control replication traffic over WAN links

To protect the root domain (and the Enterprise Admins group)

PTS: 1 REF: 15

5. List the domain functional levels that a target domain can be operating in when using ADMT v3.1.

ANS:
Windows Server 2000 Native

Windows Server 2003

Windows Server 2008

PTS: 1 REF: 26

6. How is the migration of objects handled between domains?

ANS:
Migration of objects is handled a little differently depending on whether the objects are being migrated between domains in separate forests or migrated between domains in the same forest. These two types of migrations are referred to as interforest and intraforest migrations.

Interforest migration. Objects are migrated between domains in separate forests.
Intraforest migration. Objects are migrated between domains in the same forest.

PTS: 1 REF: 27

7. Discuss the security risk of SID history if you are migrating accounts between forests that aren't completely trusted.

ANS:
While SID history is a useful feature in a fully trusted environment, it can present a security risk if you are migrating accounts between forests that aren't completely trusted. Here's the risk. If an attacker obtains SID history data, he can assign these SIDs to the SID history attributed to accounts he creates in his own domain. These new accounts will now have access to resources based on the SIDs listed in SID history.

PTS: 1 REF: 28

8. Discuss what happens when SID filtering is disabled.

ANS:
When SID filtering is disabled, it removes the security boundary between the forests and eliminates any isolation that previously existed.

PTS: 1 REF: 29

9. List the extra steps that must be taken to allow SID history to work between different forests.

ANS:
The extra steps are:
• Create a domain local group in the source domain named netBiOSDomainName$$$. For example, in CT.com, you'd create a group named CT$$$ because the NetBIOS name of CT.com is CT.
• Modify the registry of the PDC emulator on the source domain. Create a DWord value of TcpipClientSupport (or modify it if it already exists) in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA subkey. Set the value to 1.
• Enable Success and Failure for Account Management in the Default Domain Controller Policy of both the source and target domains.
• Install and configure the Password Export Server (PES) service tool.

PTS: 1 REF: 33

10. List the trusts that can be used to create a trust relationship in order to run ADMT.

ANS:
A trust between two domains in the same forest (which can be a direct parent-child trust or a transitive trust)

An external trust between two domains in different forests

A forest trust between two separate forests

PTS: 1 REF: 33