Lesson 5

Active Directory Administration

Knowledge Assessment

Fill in the Blank

1. A(n) \_global group\_ can only contain members from within the same domain. P105

2. You can use the \_\_CSVDE\_\_ utility to import data from Comma-Separated Values (CSV) files.P114

3. Each user and group object has a(n) \_SAM account name\_, which must be unique across an entire Active Directory domain.P118

4. The Anonymous Logon group is an example of a(n) \_special identity group\_.P111

5. You can use the \_\_LDIFDE\_\_ command-line utility to create and modify Active Directory objects. P114

6. When users log on to Active Directory, they receive a(n) \_access token\_ consisting of all of their security group memberships. P103

7. A local user is stored in the \_\_Security Account Manager (SAM)\_\_ database of the computer on which it was created. P102

8. Each CSV file needs to begin with a(n) \_\_header record\_\_ when used with the CSVDE command-line tool. P119

9. A(n) \_\_distribution group\_\_ can only be used to send and receive email, not to secure network resources. P104

10. \_\_Group nesting\_\_ is the practice of adding one group as a member of another group.p104

Multiple Choice

1. Which special identity group controls anonymous access to resources in Windows Server 2008?

a. Everyone

b. Network

c. Interactive

d. Anonymous Logon

Prior to Windows Server 2003, the Anonymous Logon group was a member of the Everyone group, which had the potential to create significant security liabilities. Beginning in Windows Server 2003, anonymous access must be configured separately from access granted to the Everyone group. P111

2. What defines the types of objects that can belong to a particular group and the types of resources that group can be used to secure?

a. Group scope

b. Group security

c. Special Identity group

d. Security group

The domain local group scope can contain users or groups from any domain in the forest, but can only be used to secure resources in the same domain as the group. The global group scope can contain only users or groups from the same domain as the group, but can be used to secure resources from any domain in the forest. The universal group scope can contain users or groups from any domain in the forest and can be used to secure resources in any domain in the forest. P105

3. What technique is used to configure one security group as a member of another security group?

a. Group security

b. Group nesting

c. Group overloading

d. Group scope

If GroupB is nested within GroupA, the members of GroupB will receive the same permissions that have been assigned to GroupA. P104

4. The Administrator and Guest user accounts are examples of

a. Special identity user account

b. Administrative user account

c. Built-in user account

d. Domain user account

Built-in user accounts can be local accounts or domain accounts, depending on whether you are working with a member server or an Active Directory domain controller.

5. Which command-line tool can be used to create various object types within Active Directory?

a. dsget

b. dsquery

c. dsadd

d. dsmove

Use the dsadd command-line utility to quickly create a computer, contact, group, organizational unit, user, or Active Directory quota object within an Active Directory domain. P118

6. Which input file format allows you to create, modify, and delete objects within Active Directory?

a. LDAP Data Interchange Format (LDIF)

b. Comma Separated Value (CSV)

c. Tab-delimited Text (TXT)

d. Microsoft Excel (XLS)

Unlike CSVDE, the LDIF format allows you to use the LDIFDE command-line utility to create, modify, and delete Active Directory objects. CSVDE only allows you to create objects. P114

7. Which group type allows you to assign permissions to resources, as well as receive messages via Active Directory-enabled email applications such as Microsoft Exchange?

a. Distribution group

b. Exchange group

c. Permissions group

d. Security group

Security groups serve a dual purpose in Active Directory, allowing administrators to use them to secure resources and use them as email distribution lists. Distribution groups, by contrast, can be used only for the purposes of receiving email messages. P104

8. Which group scope can contain users and groups from any domain within an Active Directory forest, but can be used only to secure resources located within the same domain as the group itself?

a. Domain group

b. Global group

c. Domain local group

d. Universal group

Following the practice of AGUDLP, the domain local group is the group scope within Active Directory that contains global or universal groups from all domains; it is actually used to secure the resource in question.P105

9. Which account type is configured on an Active Directory domain controller and can be used to grant access to resources on any domain-joined computer?

a. Domain local account

b. Global account

c. Domain account

d. Local account

Active Directory domain accounts are created and managed on domain controllers or from workstations that have the necessary administrative tools installed. Domain accounts can be used to gain access to resources domain-wide without maintaining multiple local accounts on individual computers.P102

10. What can be used to run script files using VBScript or JScript from the Windows desktop or from a command prompt?

a. Visual Basic

b. Windows Scripting Host (WSH)

c. Visual Basic Express

d. Windows Scripting Engine

The Windows Scripting Host (WSH) uses the wscript.exe runtime program to run scripts using the Windows desktop graphical user interface and script.exe to use a command-line interface. P115

Case Scenarios

Scenario 5-1: Administering Groups for Humongous Insurance

You are a network administrator for Humongous Insurance. Humongous Insurance has a multidomain forest. The forest root is humongousinsurance.com. There are also two child domains named west.humongousinsurance.com and east.humongousinsurance.com. The company has approximately 7,000 users, 7,000 client workstations, and 100 servers.

All domains are Windows Server 2008 domains. The forest root domain has 10 domain controllers. Five of those domain controllers are configured as DNS servers and two are configured as global catalog servers. The West domain has three domain controllers. Two of those domain controllers are configured as DNS servers. One of those domain controllers is configured as a global catalog server. The East domain has two Windows Server 2008 domain controllers and three Windows 2003 domain controllers.

The forest root domain is located in College Station, Texas. The East domain is located in Gainesville, Florida. The West domain is located in San Diego, California. An Active Directory site is configured for each of these locations. The site for College Station is named Main\_Site. The Gainesville site is named East\_Site. The San Diego site is named West\_Site.

You are one of several network administrators assigned to handle the forest root domain and College Station site. Your manager, Jean Trenary, has called a meeting of all network and desktop administrators. She wants to address several issues.

1. Jean says four internal auditors are in the forest root domain. Two internal auditors are in each of the child domains. Each set of internal auditors has been placed in a global group within each domain. These groups are named IA\_Main, IA\_East, and IA\_West after their respective locations. Jean wants all of the members of these groups to be able to access a common set of resources in the Main domain, while still segregating the auditors' ability to access other resources in domains other than their own. What is the recommended way to configure the groups to allow the desired functionality?

 Create a universal group in the Main domain and add all three global groups to this universal group. Create a domain local group in the Main domain and add the universal group to this domain local group. Assign permissions to the common resources to the domain local group.

2. The network administrators from the West domain want to know why everyone always recommends placing global groups into universal groups, instead of placing the users directly into the universal groups. What should you tell them?

 Every change to a universal group is replicated to a global catalog server, which increases replication traffic if users are routinely placed directly into universal groups. By placing global groups into universal groups, the membership of the universal group rarely changes, greatly reducing impact on replication traffic.

3. Jean approves a plan to hire assistants for each domain to create and manage user accounts. How can you give the assistants the immediate ability to help in this way, without making them domain administrators?

 Use the Delegation of Control Wizard to delegate the permissions to perform specific tasks, such as creating and managing user accounts.

4. Two employees have been hired to back up data and manage printers for the Main\_Site. Which built-in groups will give these users the permissions they require to manage the domain controllers? How should you set up their accounts and group memberships?

 Add the users to the Backup Operators and Print Operators groups to allow them to perform these tasks.

Scenario 5-2: Evaluating Scripts

This scenario will help you to find and evaluate one of the script types discussed in this lesson.

1. Describe each type of scripting that can add users to Active Directory. Provide an example of a scenario using each one.

 Use a batch script to combine multiple command-line tools into a single step, such as running dsadd three times in a row to create three separate user accounts.

 Use csvde to export Active Directory information, either to create a report of object information or to export it to another type of system, such as a UNIX system.

 Use lfidfe if you need a more flexible import and export option than CSVDE, because CSVDE doesn't allow you to configure attributes, such as user passwords.

 Use the WSH to automate a large number of administrative tasks, including configuring printers, creating users, and mapping network drives.

2. Using the Internet as your resource, find an example of one of the script types and write a short description of the script and what it accomplishes.

The following script is one example:

**CreateUsers.vbs**

VBScript program to create users according to the information in a ' Microsoft Excel spreadsheet.

---------------------------------------------------------------------

Copyright (c) 2003 Richard L. Mueller

Hilltop Lab web site - <http://www.rlmueller.net> ' Version 1.0 - September 8, 2003 ' Version 1.1 - January 25, 2004 - Modify error trapping.

Version 1.2 - March 18, 2004 - Modify NameTranslate constants.

Version 2.0 - October 7, 2007 - Specify container for each user object in spreadsheet. Accept NT names of groups.

Dim objExcel, strExcelPath, objSheet

Dim strLast, strFirst, strMiddle, strPW, intRow, intCol Dim strGroupDN, objUser, objGroup, objContainer Dim strCN, strNTName, strContainerDN Dim strHomeFolder, strHomeDrive, objFSO, objShell Dim intRunError, strNetBIOSDomain, strDNSDomain Dim objRootDSE, objTrans, strLogonScript, strUPN Dim strPreviousDN, blnBound

' Constants for the NameTranslate object.

Const ADS\_NAME\_INITTYPE\_GC = 3

Const ADS\_NAME\_TYPE\_NT4 = 3

Const ADS\_NAME\_TYPE\_1779 = 1

' Specify spreadsheet.

strExcelPath = "c:\MyFolder\NewUsers.xls"

Set objFSO = CreateObject("Scripting.FileSystemObject")

Set objShell = CreateObject("Wscript.Shell")

' Determine DNS domain name from RootDSE object.

Set objRootDSE = GetObject("LDAP://RootDSE") strDNSDomain = objRootDSE.Get("DefaultNamingContext")

' Use the NameTranslate object to find the NetBIOS domain name ' from the DNS domain name.

Set objTrans = CreateObject("NameTranslate") objTrans.Init ADS\_NAME\_INITTYPE\_GC, ""

objTrans.Set ADS\_NAME\_TYPE\_1779, strDNSDomain strNetBIOSDomain = objTrans.Get(ADS\_NAME\_TYPE\_NT4) ' Remove trailing backslash.

strNetBIOSdomain = Left(strNetBIOSDomain, Len(strNetBIOSDomain) - 1)

' Open spreadsheet.

Set objExcel = CreateObject("Excel.Application")

On Error Resume Next

objExcel.Workbooks.Open strExcelPath

If (Err.Number <> 0) Then

 On Error GoTo 0

 Wscript.Echo "Unable to open spreadsheet " & strExcelPath

 Wscript.Quit

End If

On Error GoTo 0

Set objSheet = objExcel.ActiveWorkbook.Worksheets(1)

' Start with row 2 of spreadsheet.

' Assume first row has column headings.

intRow = 2

' Read each row of spreadsheet until a blank value ' encountered in column 6 (the column for cn).

' For each row, create user and set attribute values.

strPreviousDN = ""

Do While objSheet.Cells(intRow, 6).Value <> ""

 ' Read values from spreadsheet for this user.

 strContainerDN = Trim(objSheet.Cells(intRow, 1).Value)

 strFirst = Trim(objSheet.Cells(intRow, 2).Value)

 strMiddle = Trim(objSheet.Cells(intRow, 3).Value)

 strLast = Trim(objSheet.Cells(intRow, 4).Value)

 strPW = Trim(objSheet.Cells(intRow, 5).Value)

 strCN = Trim(objSheet.Cells(intRow, 6).Value)

 strNTName = Trim(objSheet.Cells(intRow, 7).Value)

 strUPN = Trim(objSheet.Cells(intRow, 8).Value)

 strHomeFolder = Trim(objSheet.Cells(intRow, 9).Value)

 strHomeDrive = Trim(objSheet.Cells(intRow, 10).Value)

 strLogonScript = Trim(objSheet.Cells(intRow, 11).Value)

 ' If this container is different from the previous, bind to

 ' the container the user object will be created in.

 If (strContainerDN <> strPreviousDN) Then

 On Error Resume Next

 Set objContainer = GetObject("LDAP://" & strContainerDN)

 If (Err.Number <> 0) Then

 On Error GoTo 0

 Wscript.Echo "Unable to bind to container: " & strContainerDN

 Wscript.Echo "Unable to create user with NT name: " & strNTName

 ' Flag that container not bound.

 strPreviousDN = ""

 Else

 On Error GoTo 0

 strPreviousDN = strContainerDN

 End If

 End If

 ' Proceed if parent container bound.

 If (strPreviousDN <> "") Then

 ' Create user object.

 On Error Resume Next

 Set objUser = objContainer.Create("user", "cn=" & strCN)

 If (Err.Number <> 0) Then

 On Error GoTo 0

 Wscript.Echo "Unable to create user with cn: " & strCN

 Else

 On Error GoTo 0

 ' Assign mandatory attributes and save user object.

 If (strNTName = "") Then

 strNTName = strCN

 End If

 objUser.sAMAccountName = strNTName

 On Error Resume Next

 objUser.SetInfo

 If (Err.Number <> 0) Then

 On Error GoTo 0

 Wscript.Echo "Unable to create user with NT name: " & strNTName

 Else

 ' Set password for user.

 objUser.SetPassword strPW

 If (Err.Number <> 0) Then

 On Error GoTo 0

 Wscript.Echo "Unable to set password for user " & strNTName

 End If

 On Error GoTo 0

 ' Enable the user account.

 objUser.AccountDisabled = False

 If (strFirst <> "") Then

 objUser.givenName = strFirst

 End If

 ' Assign values to remaining attributes.

 If (strMiddle <> "") Then

 objUser.initials = strMiddle

 End If

 If (strLast <> "") Then

 objUser.sn = strLast

 End If

 If (strUPN <> "") Then

 objUser.userPrincipalName = strUPN

 End If

 If (strHomeDrive <> "") Then

 objUser.homeDrive = strHomeDrive

 End If

 If (strHomeFolder <> "") Then

 objUser.homeDirectory = strHomeFolder

 End If

 If (strLogonScript <> "") Then

 objUser.scriptPath = strLogonScript

 End If

 ' Set password expired. Must be changed on next logon.

 objUser.pwdLastSet = 0

 ' Save changes.

 On Error Resume Next

 objUser.SetInfo

 If (Err.Number <> 0) Then

 On Error GoTo 0

 Wscript.Echo "Unable to set attributes for user with NT name: " \_

 & strNTName

 End If

 On Error GoTo 0

 ' Create home folder.

 If (strHomeFolder <> "") Then

 If (objFSO.FolderExists(strHomeFolder) = False) Then

 On Error Resume Next

 objFSO.CreateFolder strHomeFolder

 If (Err.Number <> 0) Then

 On Error GoTo 0

 Wscript.Echo "Unable to create home

folder: " & strHomeFolder

 End If

 On Error GoTo 0

 End If

 If (objFSO.FolderExists(strHomeFolder) = True) Then

 ' Assign user permission to home folder.

 intRunError = objShell.Run("%COMSPEC% /c Echo

Y| cacls " \_

 & strHomeFolder & " /T /E /C /G " & strNetBIOSDomain \_

 & "\" & strNTName & ":F", 2, True)

 If (intRunError <> 0) Then

 Wscript.Echo "Error assigning permissions for user " \_

 & strNTName & " to home folder " & strHomeFolder

 End If

 End If

 End If

 ' Group DN's start in column 12.

 intCol = 12

 Do While objSheet.Cells(intRow, intCol).Value <> ""

 strGroupDN = Trim(objSheet.Cells(intRow, intCol).Value)

 ' Attempt to bind to group object DN.

 blnBound = False

 On Error Resume Next

 Set objGroup = GetObject("LDAP://" & strGroupDN)

 If (Err.Number <> 0) Then

 On Error GoTo 0

 ' Try again converting NT Name to DN.

 On Error Resume Next

 objTrans.Set ADS\_NAME\_TYPE\_NT4, strNetBIOSDomain \_

 & "\" & strGroupDN

 If (Err.Number <> 0) Then

 On Error GoTo 0

 Wscript.Echo "Unable to bind to group " & strGroupDN

 Else

 On Error GoTo 0

 strGroupDN = objTrans.Get(ADS\_NAME\_TYPE\_1779)

 Set objGroup = GetObject("LDAP://" & strGroupDN)

 blnBound = True

 End If

 Else

 On Error GoTo 0

 blnBound = True

 End If

 If (blnBound = True) Then

 objGroup.Add objUser.AdsPath

 If (Err.Number <> 0) Then

 On Error GoTo 0

 Wscript.Echo "Unable to add user " & strNTName \_

 & " to group " & strGroupDN

 End If

 End If

 On Error GoTo 0

 ' Increment to next group DN.

 intCol = intCol + 1

 Loop

 End If

 End If

 End If

 ' Increment to next user.

 intRow = intRow + 1

Loop

Wscript.Echo "Done"

' Clean up.

objExcel.ActiveWorkbook.Close

objExcel.Application.Quit

Set objUser = Nothing

Set objGroup = Nothing

Set objContainer = Nothing

Set objSheet = Nothing

Set objExcel = Nothing

Set objFSO = Nothing

Set objShell = Nothing

Set objTrans = Nothing

Set objRootDSE = Nothing