Content of List the System Access Control List for a Group.vbs (Site 1)

```
' Description: Returns information found on the System Access Control List (SACL) for an Active Directory security group named Scientists.


Const SE_SACL_PROTECTED = &H2000
Const ADS_SECURITY_INFO_OWNER = &H1
Const ADS_SECURITY_INFO_GROUP = &H2
Const ADS_OPTION_SECURITY_MASK =&H3
Const ADS_SECURITY_INFO_DACL = &H4
Const ADS_SECURITY_INFO_SACL = &H8

Set objGroup = GetObject _
   ("LDAP://cn=Scientists,ou=R&D,dc=NA,dc=fabrikam,dc=com")

objGroup.SetOption ADS_OPTION_SECURITY_MASK, ADS_SECURITY_INFO_OWNER _
   Or ADS_SECURITY_INFO_GROUP Or ADS_SECURITY_INFO_DACL _
   Or ADS_SECURITY_INFO_SACL

Set objNtSecurityDescriptor = objGroup.Get("ntSecurityDescriptor")

intNtSecurityDescriptorControl = objNtSecurityDescriptor.Control

WScript.Echo "Auditing Tab"
strMessage = "Allow inheritable auditing entries from" & _
   "the parent to "
strMessage = strMessage & "propogate to this object and all child objects "

If (intNtSecurityDescriptorControl And SE_SACL_PROTECTED) Then
   Wscript.Echo strMessage & "is disabled."
Else
   WScript.Echo strMessage & "is enabled."
End If
WScript.Echo

Set objSacl = objNtSecurityDescriptor.SystemAcl
DisplayAceInformation objSacl, "SACL"

Sub DisplayAceInformation(SecurityStructure, strType)
   Const ADS_ACETYPE_SYSTEM_AUDIT = &H2
   Const ADS_ACETYPE_SYSTEM_AUDIT_OBJECT = &H7

   intAceCount = 0
   For Each objAce In SecurityStructure
      strTrustee = Mid(objAce.Trustee,1,12)
      If StrComp(strTrustee, "NT AUTHORITY", 1) <> 0 Then
         intAceCount = intAceCount + 1
         WScript.Echo strType & " permission entry: " & intAceCount
         WScript.Echo "Name: " & objAce.Trustee

         intAceType = objAce.AceType
         WScript.Echo "ACETYPE IS: " & intAceType
         If (intAceType = ADS_ACETYPE_SYSTEM_AUDIT or _
            intAceType = ADS_ACETYPE_SYSTEM_AUDIT_OBJECT) Then
            WScript.Echo "Type: Success or Failure Audit"
         Else
            WScript.Echo "Audit Type Unknown."
         End If
         ReadBitsInAccessMask(objAce.AccessMask)
         WScript.Echo
      End If
   Next
End Sub

Sub ReadBitsInAccessMask(AccessMask)
   Const ADS_RIGHT_DELETE = &H10000
   Const ADS_RIGHT_READ_CONTROL = &H20000
   Const ADS_RIGHT_WRITE_DAC = &H40000
   Const ADS_RIGHT_WRITE_OWNER = &H80000
   Const ADS_RIGHT_DS_CREATE_CHILD = &H1
   Const ADS_RIGHT_DS_DELETE_CHILD = &H2
   Const ADS_RIGHT_ACTRL_DS_LIST = &H4
   Const ADS_RIGHT_DS_SELF = &H8
   Const ADS_RIGHT_DS_READ_PROP = &H10
   Const ADS_RIGHT_DS_WRITE_PROP = &H20
   Const ADS_RIGHT_DS_DELETE_TREE = &H40
   Const ADS_RIGHT_DS_LIST_OBJECT = &H80
   Const ADS_RIGHT_DS_CONTROL_ACCESS = &H100

   WScript.Echo VbCrLf & "Standard Access Rights"
   If (AccessMask And ADS_RIGHT_DELETE) Then _
      WScript.Echo vbTab & "-Delete an object."
   If (AccessMask And ADS_RIGHT_READ_CONTROL) Then _
      WScript.Echo vbTab & "-Read permissions."
   If (AccessMask And ADS_RIGHT_WRITE_DAC) Then _
      WScript.Echo vbTab & "-Write permissions."
   If (AccessMask And ADS_RIGHT_WRITE_OWNER) Then _
      WScript.Echo vbTab & "-Modify owner."

   WScript.Echo VbCrLf & "Directory Service Specific Access Rights"
   If (AccessMask And ADS_RIGHT_DS_CREATE_CHILD) Then _
      WScript.Echo vbTab & "-Create child objects."
   If (AccessMask And ADS_RIGHT_DS_DELETE_CHILD) Then _
      WScript.Echo vbTab & "-Delete child objects."
   If (AccessMask And ADS_RIGHT_ACTRL_DS_LIST) Then _
      WScript.Echo vbTab & "-Enumerate an object."
   If (AccessMask And ADS_RIGHT_DS_READ_PROP) Then _
      WScript.Echo vbTab & "-Read the properties of an object."
   If (AccessMask And ADS_RIGHT_DS_WRITE_PROP) Then _
      WScript.Echo vbTab & "-Write the properties of an object."
   If (AccessMask And ADS_RIGHT_DS_DELETE_TREE) Then _
      WScript.Echo vbTab & "-Delete a tree of objects"
   If (AccessMask And ADS_RIGHT_DS_LIST_OBJECT) Then _
      WScript.Echo vbTab & "-List a tree of objects."

   WScript.Echo VbCrLf & "Control Access Rights"
   If (AccessMask And ADS_RIGHT_DS_CONTROL_ACCESS) + _
      (AccessMask And ADS_RIGHT_DS_SELF) = 0 Then
         WScript.Echo "-None"
   Else
      If (AccessMask And ADS_RIGHT_DS_CONTROL_ACCESS) Then _
         WScript.Echo vbTab & "-Extended access rights."
      If (AccessMask And ADS_RIGHT_DS_SELF) Then
         WScript.Echo vbTab & "-Active Directory must validate a property "
         WScript.Echo vbTab & " write operation beyond the schema " & _
            "definition "
         WScript.Echo vbTab & " for the attribute."
      End If
   End If
End Sub
```