Content of List the Security Descriptor for an OU.vbs (Site 1)

```
' Description: Returns the information found on the security descriptor for the Sales OU in Active Directory.


Const SE_DACL_PROTECTED = &H1000

Set objContainer = GetObject _
  ("LDAP://ou=Sales,dc=NA,dc=fabrikam,dc=com")

Set objNtSecurityDescriptor = objContainer.Get("ntSecurityDescriptor")

intNtSecurityDescriptorControl = objNtSecurityDescriptor.Control

WScript.Echo "Permissions Tab"
strMessage = "Allow inheritable permissions from the parent to " & _
    "propogate to this object and all child objects "
If (intNtSecurityDescriptorControl And SE_DACL_PROTECTED) Then
    Wscript.Echo strMessage & "is disabled."
Else
    WScript.Echo strMessage & "is enabled."
End If
WScript.Echo

Set objDiscretionaryAcl = objNtSecurityDescriptor.DiscretionaryAcl
DisplayAceInformation objDiscretionaryAcl, "DACL"

Sub DisplayAceInformation(SecurityStructure, strType)
    Const ADS_ACETYPE_ACCESS_ALLOWED = &H0
    Const ADS_ACETYPE_ACCESS_DENIED = &H1
    Const ADS_ACETYPE_ACCESS_ALLOWED_OBJECT = &H5
    Const ADS_ACETYPE_ACCESS_DENIED_OBJECT = &H6
    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
            If (intAceType = ADS_ACETYPE_ACCESS_ALLOWED Or _
                intAceType = ADS_ACETYPE_ACCESS_ALLOWED_OBJECT) Then
                WScript.Echo "Type: Allow Access"
            ElseIf (intAceType = ADS_ACETYPE_ACCESS_DENIED Or _
                intAceType = ADS_ACETYPE_ACCESS_DENIED_OBJECT) Then
                WScript.Echo "Type: Deny Acess"
            Else
                WScript.Echo "Acess Type Unknown."
            End If
            ReadBitsInAccessMask(objAce.AccessMask)
            WScript.Echo VbCr
        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
```

This document was created by www.scriptbox.at.tt (http://scriptbox.boris-toll.at) -> Boris TOLL