

```
1 ' -----
2 '     From the book Inside Active Directory, ISBN 0-201-61621-1
3 '     Copyright (C) 2002 by Addison-Wesley
4 '     Script by Sakari Kouti (see http://www.kouti.com)
5 ' You have a royalty-free right to use, modify, reproduce and distribute
6 ' this script (and/or any modified version) in any way you find useful,
7 ' provided that you agree that Addison-Wesley or Sakari Kouti has no
8 ' warranty, obligations or liability for the script. If you modify
9 ' the script, you must retain this copyright notice.
10 ' -----
11 Option Explicit
12
13 'AccessMask Bits
14 'Constants would be like ADS_RIGHT_DS_CREATE_CHILD
15 Dim arrADSRights(18,1) '19 value pairs, name and bit in each
16 arrADSRights(0,0) = "DS_CREATE_CHILD"
17 arrADSRights(0,1) = &H1
18 arrADSRights(1,0) = "DS_DELETE_CHILD"
19 arrADSRights(1,1) = &H2
20 arrADSRights(2,0) = "ACTRL_DS_LIST"
21 arrADSRights(2,1) = &H4
22 arrADSRights(3,0) = "DS_SELF"
23 arrADSRights(3,1) = &H8
24 arrADSRights(4,0) = "DS_READ_PROP"
25 arrADSRights(4,1) = &H10
26 arrADSRights(5,0) = "DS_WRITE_PROP"
27 arrADSRights(5,1) = &H20
28 arrADSRights(6,0) = "DS_DELETE_TREE"
29 arrADSRights(6,1) = &H40
30 arrADSRights(7,0) = "DS_LIST_OBJECT"
31 arrADSRights(7,1) = &H80
32 arrADSRights(8,0) = "DS_CONTROL_ACCESS"
33 arrADSRights(8,1) = &H100
34 arrADSRights(9,0) = "DELETE"
35 arrADSRights(9,1) = &H10000
36 arrADSRights(10,0) = "READ_CONTROL"
37 arrADSRights(10,1) = &H20000
38 arrADSRights(11,0) = "WRITE_DAC"
39 arrADSRights(11,1) = &H40000
40 arrADSRights(12,0) = "WRITE_OWNER"
41 arrADSRights(12,1) = &H80000
42 arrADSRights(13,0) = "SYNCHRONIZE"
43 arrADSRights(13,1) = &H100000
44 arrADSRights(14,0) = "ACCESS_SYSTEM_SECURITY"
45 arrADSRights(14,1) = &H1000000
46 arrADSRights(15,0) = "GENERIC_ALL"
47 arrADSRights(15,1) = &H10000000
48 arrADSRights(16,0) = "GENERIC_EXECUTE"
49 arrADSRights(16,1) = &H20000000
50 arrADSRights(17,0) = "GENERIC_WRITE"
51 arrADSRights(17,1) = &H40000000
52 arrADSRights(18,0) = "GENERIC_READ"
53 arrADSRights(18,1) = &H80000000
54
55 'AceFlags Bits
56 'Constants would be like ADS_ACEFLAG_INHERIT_ACE
57 Dim arrADSACEFlags(5,1) '6 value pairs, name and bit in each
58 arrADSACEFlags(0,0) = "INHERIT_ACE"
59 arrADSACEFlags(0,1) = &H2
60 arrADSACEFlags(1,0) = "NO_PROPAGATE_INHERIT_ACE"
61 arrADSACEFlags(1,1) = &H4
62 arrADSACEFlags(2,0) = "INHERIT_ONLY_ACE"
63 arrADSACEFlags(2,1) = &H8
64 arrADSACEFlags(3,0) = "INHERITED_ACE"
65 arrADSACEFlags(3,1) = &H10
66 arrADSACEFlags(4,0) = "SUCCESSFUL_ACCESS"
67 arrADSACEFlags(4,1) = &H40
68 arrADSACEFlags(5,0) = "FAILED_ACCESS"
69 arrADSACEFlags(5,1) = &H80
70
71 'AceTypes
72 'Constants would be like ADS_ACETYPE_ACCESS_ALLOWED
73 Dim arrADSACETypes(5,1) '6 value pairs, name and value in each
74 arrADSACETypes(0,0) = "ACCESS_ALLOWED"
75 arrADSACETypes(0,1) = 0
76 arrADSACETypes(1,0) = "ACCESS_DENIED"
```

```

77 arrADSACETypes(1,1) = &H1
78 arrADSACETypes(2,0) = "SYSTEM_AUDIT"
79 arrADSACETypes(2,1) = &H2
80 arrADSACETypes(3,0) = "ACCESS_ALLOWED_OBJECT"
81 arrADSACETypes(3,1) = &H5
82 arrADSACETypes(4,0) = "ACCESS_DENIED_OBJECT"
83 arrADSACETypes(4,1) = &H6
84 arrADSACETypes(5,0) = "SYSTEM_AUDIT_OBJECT"
85 arrADSACETypes(5,1) = &H7
86
87 'Flags Bits
88 'Constants would be like ADS_FLAG_OBJECT_TYPE_PRESENT
89 Dim arrADSFlags(1,1) '2 value pairs, name and bit in each
90 arrADSFlags(0,0) = "OBJECT_TYPE_PRESENT"
91 arrADSFlags(0,1) = &H1
92 arrADSFlags(1,0) = "INHERITED_OBJECT_TYPE_PRESENT"
93 arrADSFlags(1,1) = &H2
94
95 Dim objDSE, strDefaultDN, strDN, objADObject, i
96 Dim objSecDesc, objDAcl, objACE
97
98 '===The Main Program===
99
100 Set objDSE = GetObject("LDAP://rootDSE")
101 strDefaultDN = "CN=Users," & objDSE.Get("defaultNamingContext")
102
103 strDN = InputBox("Enter the distinguished name of an object" & _
104 vbCrLf & "(e.g. " & strDefaultDN & ")", , strDefaultDN)
105
106 If strDN = "" Then WScript.Quit(0) 'user clicked Cancel
107
108 Set objADObject = GetObject("LDAP://" & strDN)
109
110 Set objSecDesc = objADObject.Get("ntSecurityDescriptor")
111 Set objDAcl = objSecDesc.DiscretionaryAcl
112
113 WScript.Echo "Number of ACEs: " & objDAcl.AceCount
114
115 i = 0
116 For Each objACE In objDAcl
117     i = i + 1
118     WScript.Echo ""
119     WScript.Echo "ACE " & i
120     WScript.Echo "Trustee: " & objACE.Trustee
121     WScript.Echo GetStringBits("AccessMask", _
122         objACE.AccessMask, arrADSRights)
123     WScript.Echo GetStringBits("AceFlags", _
124         objACE.AceFlags, arrADSACEFlags)
125     WScript.Echo GetStringAceType(objACE.AceType)
126     WScript.Echo GetStringBits("Flags", _
127         objACE.Flags, arrADSFlags)
128     WScript.Echo GetObjectType(objACE.ObjectType)
129     WScript.Echo GetInheritedObjectType(objACE.InheritedObjectType)
130 Next
131
132 '===End of the Main Program===
133 '=====
134
135 Function GetStringBits(strName, intBitfield, arrBits)
136     Dim strOut, i
137
138     strOut = strName & ": " & Hex(intBitfield)
139
140     For i = LBound(arrBits) To UBound(arrBits)
141         If intBitfield And arrBits(i,1) Then
142             strOut = strOut & ", " & arrBits(i,0)
143         End If
144     Next
145
146     GetStringBits = strOut
147 End Function
148
149 '=====
150
151 Function GetStringAceType(intACEType)
152     Dim strOut, i

```

```

153
154     strOut = "unknown ACE type"
155     For i = LBound(arrADSACETypes) To UBound(arrADSACETypes)
156         If intACEType = arrADSACETypes(i,1) Then
157             strOut = arrADSACETypes(i,0)
158         End If
159     Next
160
161     GetStringAceType = "AceType: " & Hex(intACEType) & ", " & strOut
162 End Function
163
164 '=====
165
166 Function GetObjectType(strGUID)
167     GetObjectType = "ObjectType: " & _
168         strGUID & " " & MapGUIDToMatchingName(strGUID)
169 End Function
170
171 '=====
172
173 Function GetInheritedObjectType(strGUID)
174     GetInheritedObjectType = "InheritedObjectType: " & _
175         strGUID & " " & MapGUIDToMatchingName(strGUID)
176 End Function
177
178 '=====
179
180 Function MapGUIDToMatchingName(strGUIDAsString)
181     Dim strOut, objExtRights, objChild, objSchema
182
183     If strGUIDAsString = "" Then Exit Function
184
185     strOut = ""
186
187     Set objExtRights = GetObject("LDAP://CN=Extended-Rights," & _
188         objDSE.Get("configurationNamingContext"))
189
190     For Each objChild In objExtRights
191         'Actually all should be of the same class
192         If objChild.Class = "controlAccessRight" Then
193             If UCase("{ " & objChild.Get("rightsGuid") & "}") = _
194                 UCase(strGUIDAsString) Then
195                 strOut = objChild.Get("cn") & ":" & _
196                     objChild.Get("displayName")
197             Exit For
198         End If
199     End If
200 Next
201
202     If strOut = "" Then 'Didn't find a match in extended rights
203         Set objSchema = GetObject("LDAP://" & _
204             objDSE.Get("schemaNamingContext"))
205
206         For Each objChild In objSchema
207             If objChild.Class = "classSchema" Or _
208                 objChild.Class = "attributeSchema" Then
209                 If UCase(GetSchemaIDGUID(objChild)) = _
210                     UCase(strGUIDAsString) Then
211                     strOut = objChild.Get("cn") & ":" & _
212                         objChild.Get("LDAPDisplayName")
213                 Exit For
214             End If
215         End If
216     Next
217 End If
218
219     MapGUIDToMatchingName = strOut
220 End Function
221
222 '=====
223
224 Function GetSchemaIDGUID(objSchemaObj)
225     Dim arrValue, i, strByte, strGUID
226
227     arrValue = objSchemaObj.Get("schemaIDGUID")
228     strGUID = ""

```

```
229     For i = 1 to LenB(arrValue)
230         strByte = Hex(AscB(MidB(arrValue, i, 1)))
231         If Len(strByte) = 1 Then strByte = "0" & strByte
232         strGUID = strGUID & strByte
233     Next
234     GetSchemaIDGUID = GuidBinFormatToStrFormat(strGUID)
235 End Function
236
237 '=====
238
239 Function GUIDBinFormatToStrFormat(strGUIDBin)
240     Dim i, strDest
241     Dim arrBytes(16)           'We will use elements 1 to 16 but not 0
242
243     For i = 1 To 16     'A GUID has 16 bytes
244         arrBytes(i) = Mid(strGUIDBin, 2 * i - 1, 2)
245     Next
246
247     strDest = "{"
248     For i = 1 To 4 : strDest = strDest & arrBytes(5 - i) : Next
249     strDest = strDest & "-"
250     For i = 1 To 2 : strDest = strDest & arrBytes(7 - i) : Next
251     strDest = strDest & "-"
252     For i = 1 To 2 : strDest = strDest & arrBytes(9 - i) : Next
253     strDest = strDest & "-"
254     For i = 1 To 2 : strDest = strDest & arrBytes(8 + i) : Next
255     strDest = strDest & "-"
256     For i = 1 To 6 : strDest = strDest & arrBytes(10 + i) : Next
257     strDest = strDest & "}"
258
259     GuidBinFormatToStrFormat = strDest
260 End Function
261
```