```
' ----------------------------------------------------------------------
'       From the book Inside Active Directory, ISBN 0-201-61621-1
'       Copyright (C) 2002 by Addison-Wesley
'       Script by Sakari Kouti (see http://www.kouti.com)
' You have a royalty-free right to use, modify, reproduce and distribute
' this script (and/or any modified version) in any way you find useful,
' provided that you agree that Addison-Wesley or Sakari Kouti has no
' warranty, obligations or liability for the script. If you modify
' the script, you must retain this copyright notice.
' ----------------------------------------------------------------------
Option Explicit

'AccessMask
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
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_SYNCHRONIZE             = &H100000
Const ADS_RIGHT_ACCESS_SYSTEM_SECURITY = &H1000000
Const ADS_RIGHT_GENERIC_ALL             = &H10000000
Const ADS_RIGHT_GENERIC_EXECUTE         = &H20000000
Const ADS_RIGHT_GENERIC_WRITE           = &H40000000
Const ADS_RIGHT_GENERIC_READ            = &H80000000

Const ADS_RIGHT_FULL_CONTROL = &HF01FF

'ACE flags
Const ADS_ACEFLAG_INHERIT_ACE = &H2
Const ADS_ACEFLAG_NO_PROPAGATE_INHERIT_ACE = &H4
Const ADS_ACEFLAG_INHERIT_ONLY_ACE = &H8
Const ADS_ACEFLAG_INHERITED_ACE = &H10
Const ADS_ACEFLAG_SUCCESSFUL_ACCESS = &H40
Const ADS_ACEFLAG_FAILED_ACCESS = &H80

'ACE types
Const ADS_ACETYPE_ACCESS_ALLOWED            = 0
Const ADS_ACETYPE_ACCESS_DENIED             = &H1
Const ADS_ACETYPE_SYSTEM_AUDIT              = &H2
Const ADS_ACETYPE_ACCESS_ALLOWED_OBJECT     = &H5
Const ADS_ACETYPE_ACCESS_DENIED_OBJECT      = &H6
Const ADS_ACETYPE_SYSTEM_AUDIT_OBJECT       = &H7

'Flags
Const ADS_FLAG_OBJECT_TYPE_PRESENT            = &H1
Const ADS_FLAG_INHERITED_OBJECT_TYPE_PRESENT = &H2

'Some schemaIDGUIDs
Const SCHEMAIDGUID_USER = _
    "{BF967ABA-0DE6-11D0-A285-00AA003049E2}"
Const SCHEMAIDGUID_GROUP = _
    "{BF967A9C-0DE6-11D0-A285-00AA003049E2}"
Const SCHEMAIDGUID_COMPUTER = _
    "{BF967A86-0DE6-11D0-A285-00AA003049E2}"
Const SCHEMAIDGUID_CONTACT = _
    " {5CB41ED0-0E4C-11D0-A286-00AA003049E2}"
Const SCHEMAIDGUID_OU = _
    "{BF967AA5-0DE6-11D0-A285-00AA003049E2}"
Const SCHEMAIDGUID_PRINTER = _
    "{BF967AA8-0DE6-11D0-A285-00AA003049E2}"

Dim objDSE, objDom, objOU, objSecDesc, objDACL
Dim objACE1, objACE2, objACE3

'======================

'Create the OU
'---------------------------
```

```
77  Set objDSE = GetObject("LDAP://rootDSE")
78  Set objDom = GetObject("LDAP://" & _
79      objDSE.Get("defaultNamingContext"))
80  Set objOU = objDom.Create("organizationalUnit", "OU=ACEDemo")
81  objOU.SetInfo
82
83  'Create the first ACE - write all properties of the OU
84  '-----------------------------------------------------------
85  Set objACE1 = CreateObject("AccessControlEntry")
86  objACE1.Trustee         = "Red.Baron@sanao.com"
87  objACE1.AccessMask      = ADS_RIGHT_DS_WRITE_PROP
88  objACE1.AceFlags        = 0 'no inheritance from up or to below
89  objACE1.AceType         = ADS_ACETYPE_ACCESS_ALLOWED
90  objACE1.Flags           = 0 'no object types present
91  'objACE1.ObjectType     = not used
92  'objACE1.InheritedObjectType = not used
93
94  'Create the second ACE - Full Control to user objects in the subtree
95  '-------------------------------------------------------------------------
96  Set objACE2 = CreateObject("AccessControlEntry")
97  objACE2.Trustee         =   "Red.Baron@sanao.com"
98  objACE2.AccessMask      =   ADS_RIGHT_FULL_CONTROL  'all 13 bits
99  objACE2.AceFlags        =   ADS_ACEFLAG_INHERIT_ACE + _
100                              ADS_ACEFLAG_INHERIT_ONLY_ACE
101 objACE2.AceType         =   ADS_ACETYPE_ACCESS_ALLOWED_OBJECT
102 objACE2.Flags           =   ADS_FLAG_INHERITED_OBJECT_TYPE_PRESENT
103 'objACE2.ObjectType     =   not used
104 objACE2.InheritedObjectType = SCHEMAIDGUID_USER
105
106 'Create the third ACE - Create/Delete user objects in the subtree
107 '-------------------------------------------------------------------------
108 Set objACE3 = CreateObject("AccessControlEntry")
109 objACE3.Trustee         =   "Red.Baron@sanao.com"
110 objACE3.AccessMask      =   ADS_RIGHT_DS_CREATE_CHILD + _
111                             ADS_RIGHT_DS_DELETE_CHILD
112 objACE3.AceFlags        =   ADS_ACEFLAG_INHERIT_ACE
113 objACE3.AceType         =   ADS_ACETYPE_ACCESS_ALLOWED_OBJECT
114 objACE3.Flags           =   ADS_FLAG_OBJECT_TYPE_PRESENT
115 objACE3.ObjectType      =   SCHEMAIDGUID_USER
116 'objACE3.InheritedObjectType = not used
117
118 'Add the ACEs
119 '---------------------------
120 Set objSecDesc = objOU.Get("ntSecurityDescriptor")
121 Set objDACL = objSecDesc.DiscretionaryAcl
122
123 Call objDACL.AddAce(objACE1)
124 Call objDACL.AddAce(objACE2)
125 Call objDACL.AddAce(objACE3)
126
127 objSecDesc.DiscretionaryAcl = objDACL
128 Call objOU.Put("ntSecurityDescriptor", objSecDesc)
129 objOU.SetInfo
130
131 WScript.Echo "Number of ACEs after: " & objDACL.AceCount
132
```