ACTIVE DIRECTORY – HOW DO I FORMULATE LDAP QUERIES AND FILTERS?

CONVENTIONS AND DEFINITIONS

- ()
  - Parenthesis encapsulate filters and separate them into sections
- {}
  - Braces (or curly brackets) encapsulate my notes about the contents of the filter
- **CAPITAL LETTERS**
  - Plain English title
- **mIxEd cAsE**
  - Attribute name in AD
- **Bit Value**
  - Decimal value of a binary number (ie. 001000010 bin=34 dec). If you want to examine multiple bit values, simply add them up (ie. 2+65536=65538). Use the "**Bitwise AND**" or "**Bitwise OR**" filters for searches based on these values.
- **Attribute**
  - Attributes are the properties of an **Object** in AD.
- **Value**
  - Values are data related to the attributes with which they are associated. They may be "**present**" or "**not present**" (blank). Data may be in plain text, hex, numeric, or other formats.
- **Class**
  - Objects in **AD** are categorized into **Classes**. This document only discusses 3 classes: **Users**, **Computers**, and **Groups**.
- **Integer8 Date**
  - The value represents the number of **100-nanosecond** intervals since 12:00 AM January 1, 1601.
  - At the bottom of this document you can find the text of a **VBScript** that will convert normal dates to **Integer8** dates so that you can use them in searches. Simply cut and paste the VB into a text file with a **.vbs** extension and use it from a command prompt.
  - **NOTE**: Remember, the lower this number is the further back in time it is. Use <= for "on or before" queries.

WHERE TO GET INFORMATION

- Microsoft's MSDN website
- Google

- ADSI Edit
  - **USE EXTREME CAUTION WHEN USING THIS UTILITY. DO NOT MANUALLY CHANGE ANY VALUES WHILE USING THIS UTILITY.**
  - This utility allows you to see the actual attribute names and the values they use so that you can perform searches. This utility is included with the **Windows 2000 Server** or **Windows Server 2003** support pack.

FILTERS

******BASE FILTERS******
WILDCARD.....*
PRESENCE.....(attribute=*)
EQUALITY.....(attribute=value)
PARTIAL MATCH.....(attribute={partial value}*)
PARTIAL MATCH.....(attribute=*{partial value})
PARTIAL MATCH.....(attribute=*{partial value}*)
PARTIAL MATCH.....(attribute=*{partial value 1}*{partial value 2}*)
GREATER THAN or EQUAL.....(attribute>=value)
LESS THAN or EQUAL.....(attribute<=value)
APPROXIMATELY EQUAL.....(attribute~=value)

******BOOLEAN FILTERS******
AND.....(&(filter1)(filter2))
AND.....(&(filter1)(filter2)(filter3))
OR.....(|(filter1)(filter2))
OR.....(|(filter1)(filter2)(filter3))
NOT.....(!(filter1))
BITWISE AND.....(attribute:1.2.840.113556.1.4.803:={bitvalue in decimal})
BITWISE OR.....(attribute:1.2.840.113556.1.4.804:={bitvalue in decimal})

******SPECIAL CHARACTERS IN "VALUE" FIELDS******
(.....\28
).....\29
*.....\2A
\.....\5C

******CORRELARY FILTERs******
NOT PRESENT (BLANK FIELD).....(!(attribute=*))

COMMON OBJECT CLASSES AND ATTRIBUTES

******USER ACCOUNT******
CLASS.....objectCategory=person AND objectClass=user
ACCOUNT DISABLED.....userAccountControl={contains bit value of 2}
PASSWORD NOT REQUIRED.....userAccountControl={contains bit value of 32}
PASSWORD NEVER EXPIRES.....userAccountControl={contains bit value of 65536}
SMARTCARD REQUIRED.....userAccountControl={contains bit value of 262144}
ACCOUNT TRUSTED FOR DELEGATION.....userAccountControl={contains bit value of 524288}
ACCOUNT CANNOT BE DELEGATED.....userAccountControl={contains bit value of 1048576}
USE DES ENCRYPTION.....userAccountControl={contains bit value of 2097152}
DON'T REQUIRE KERBEROS PRE-AUTH....userAccountControl={contains bit value of 4194304}
PREVIOUS PASSWORD CHANGE.....pwdLastSet {Integer8 Date, use .vbs to convert conventional dates, use "<=" for all dates before or ">=" for all dates after}
LAST LOGON.....lastLogon {Integer8 Date as above, value of 0 or blank means NEVER}

REQUIRE P/W CHANGE AT NEXT LOGON...pwdLastSet {Value of 0, any other value is previous p/w change date}
GROUP MEMBERSHIP.....memberOf {Specify exact DN of group, no wildcards allowed}
EXCHANGE USER.....msExchHomeServerName {wildcard, or complete or partial servername}
EXCHANGE USER (OPTIONAL).....homeMDB {wildcard, or complete or partial database name}
DESCRIPTION.....description {wildcard, or complete or partial text}
FIRST NAME.....givenName {wildcard, or complete or partial text}
LAST NAME.....sn {wildcard, or complete or partial text}
EMPLOYEE TYPE.....employeeType {wildcard, or complete or partial text}
EMPLOYEE NUMBER.....employeeID {wildcard, or complete or partial text}
DEPARTMENT NUMBER.....department {wildcard, or complete or partial text}
LOGON NAME.....sAMAccountName {wildcard, or complete or partial text}
USER PRINCIPAL NAME (UPN).....userPrincipalName {wildcard, or complete or partial text}

******COMPUTER ACCOUNT******
CLASS.....objectClass=computer
OS NAME.....operatingSystem {ie. Windows 2000 Professional, use "PARTIAL" filter}
OS SERVICE PACK.....operatingSystemServicePack {ie. Service Pack 4, use "PARTIAL" filter}
OS VERSION.....operatingSystemVersion {ie. 5.0 (2195), use "PARTIAL" filter}
DOMAIN CONTROLLER.....userAccountControl={contains bit value of 8192}
ACCOUNT TRUSTED FOR DELEGATION.....userAccountControl={contains bit value of 524288}
DESCRIPTION.....description {wildcard, or complete or partial text}

******GROUP OBJECTS******
CLASS.....objectClass=group
DESCRIPTION.....description {wildcard, or complete or partial text}
NAME.....CN {wildcard, or complete or partial text}
SECURITY GROUP.....groupType {contains bit value of 2147483648}
GLOBAL GROUP.....groupType {contains bit value of 2}
DOMAIN LOCAL GROUP.....groupType {contains bit value of 4}
UNIVERSAL GROUP.....groupType {contains bit value of 8}

SAMPLE QUERY SEGMENTS

- Object is a user
  - (&(objectCategory=person)(objectClass=user))
- Account is not disabled
  - (!(userAccountControl:1.2.840.113556.1.4.803:=2))
- Object is an Enabled User
  - (&(objectCategory=person)(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
- Account is assigned an Exchange Mailbox
  - (|(homeMDB=*)(msExchHomeServerName=*))
- User is member of group (Specify exact DN of Group. Use ADSIEdit to determine if unsure.)
  - (memberOf=CN=your group name,OU=your ou,DC=yourdomain,DC=tld)
- Account Password Never Expires not set
  - (!(userAccountControl:1.2.840.113556.1.4.803:=65536))

- Password set on or before 8/9/2004 (Specify Integer8 Date, Use VB script to determine)
  - (pwdLastSet<=127365120000000000)

- Change Password at next logon flag
  - (pwdLastSet=0)

- Account has never logged on
  - (|(lastLogon=0)(!(lastLogon=*)))

SAMPLE FULL QUERIES (NOTE: If you cut and paste from this document, remove any extra carriage returns)

- [Object is an Enabled User Account] and [Has an Exchange mailbox] and [Not members of the All Mail Users D/L]
  - (&(&(&(objectCategory=person)(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))(|(homeMDB=*)(msExchHomeServerName=*)))(!(memberOf=CN=your group name,OU=your ou,DC=yourdomain,DC=tld)))

- [Object is a User Account] and [P/W never expires flag is not set and not disabled] and [P/W changed on or before 8/9/04] and [Password change flag is not set]
  - (&(&(&(&(objectCategory=person)(objectClass=user))(!(userAccountControl:1.2.840.113556.1.4.804:=65538)))(pwdLastSet<=127365120000000000))(!(pwdLastSet=0)))

- [Object is an Enabled User Account] and [P/W changed on or before 8/9/04] or [Password change flag is set and Last Logon is never] or [Last Logon is >90 days]
  - (&(&(objectCategory=person)(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))(|(&(pwdLastSet=0)(|(lastLogon=0)(!(lastLogon=*))))(lastLogon<=127439424000000000)(&(pwdLastSet<=127365120000000000)(!(userAccountControl:1.2.840.113556.1.4.803:=65536)))))

- [Object is a Group] and [type of Global and Security]
  - (&(objectClass=group)(groupType:1.2.840.113556.1.4.803:=2147483650))

- [Object is a Computer] and [P/W changed on or before 8/9/04]
  - (&(objectClass=computer)(pwdLastSet<=127365120000000000))

- [Object is a Computer] and [Is a Domain Controller] and [Is running Windows NT 4]
  - (&(&(objectClass=computer)(userAccountControl:1.2.840.113556.1.4.803:=8192))(operatingSystemVersion=4*))