Use Dynamic Groups with Active Directory Path Queries

Question

Is it possible to use an LDAP query to pare down the list of servers in my systems list in Privileged Identity tools?

Answer

Our tools make use of dynamic groups to allow for automatic addition and removal of systems from the systems list. The most flexible feature of the tool is to the Active Directory Path query tool where you can choose to query not only a particular OU for a set of systems but also create a custom LDAP query to fine tune the systems list that is automatically built for you.

For example, if you have an OU container called *servers* that contains 50 computer accounts in it and the machines have names such as *DBCLUSTER01*, *DBSRV01*, *DBSRV02*, *WEBSRV02*, etc., when our query runs we will populate your list with every system from the servers OU. This is because our default dynamic group query is:

(objectClass=computer)

This means to query for all objects that are identified as computers in Active Directory. The statement would be read as, *show all computer objects*.

Given the above example where we also have a naming convention where our database servers begin with *DB* and the web servers begin with *WEB*, if we wanted to use the AD query to include only the database systems our LDAP query would change to the following:

(&(objectClass=computer)(sAMAccountName=DB*))

This would create a list that involved all computers from the target OU where the name of the computer started with *DB*: *DBCLUSTER01*, *DBSRV01*, *DBSRV02*.... The statement would be read as, *show all computer objects whose names must begin with DB*.

Now imagine that the description of the computers or the location attribute was also defined in AD. And that you wanted to further define the list to include a portion of the description, your query would change to the following:

(&(objectClass=computer)(sAMAccountName=DB*)(descr iption=TEXTHERE))

The statement would be read as, *show all computer objects, whose names must begin with DB, and their descriptions exactly match...*

You may also exclude systems using these queries. The operator for NOT is an exclamation mark (!). To add all DB servers but exclude all systems with cluster in their name, the query would look as follows:

(&(objectClass=computer)(sAMAccountName=DB*)(!(sAM AccountName=*CLUSTER*)))

The statement would be read as, *show all computer objects whose names begin with DB but exclude those 'DB' systems with cluster in their name*.

Finally, the OR operator is the pipe (|) symbol. For example, adding all 2008 and 2003 systems to a systems list:

(&(objectClass=computer)(|(operatingSystem=*2008*) (operatingSystem=*2003*)))

The statement would be read as, *show all computer objects whose operating system is either 2008 or 2003*. Be careful with queries like this, as changing the statement to **(&(objectClass=computer)(operatingSystem=*2008*)(o peratingSystem=*2003*))** would be interpreted as *show all computers whose operating system type is 2008* ***and*** *2003*. A system would not have two operating systems types.

Queries can be much more or less complex than what is shown here. Any attribute present in Active Directory may be used for a possible query. Three additional and useful computer filters are:

- Disabled account: userAccountControl:1.2.840.113556.1.4.803:=2
- Domain Controllers: userAccountControl:1.2.840.113556.1.4.803:=8192
- Global Catalogs: (&(objectCategory=nTDSDSA)(options:1.2.840.113556. 1.4.803:=1))

To find all computers and exclude all disabled computer accounts use the following query:

(&(objectCategory=computer)(!(userAccountControl:1 .2.840.113556.1.4.803:=2)))

The LDAP attributes you use are only limited to what can be queried for in Active Directory and the syntax used is also identical.