LDAP Queries

Question

Can LDAP queries be used to scale down the list of servers in my **Systems** list?

Answer

The Privileged Identity Suite makes use of dynamic groups for the automatic addition and removal of systems from the **Systems** list. The most flexible feature is the **Active Directory Path** query tool, which allows you to query not only a specific Organizational Unit (OU) for a set of systems but also creates a custom LDAP query to fine tune the **Systems** list.

Examples

You have an OU container called *Servers*. It contains 50 computer accounts. The machines have names such as DBCLUSTER01, DBSRV01, DBSVR02, WEBSVR01, WEBSRV02, etc. When the query runs, the tool populates the list with every system from the server's OU. This behavior occurs because the default dynamic group query is:

(objectClass=computer)

To query for all objects identifying as computers in Active Directory, the statement would read *show all computer objects*.

In the example above, the naming convention for the servers was based on whether the server was a database (DB) server or a web (WEB) server. If we wanted to use the query to list only database systems, the LDAP query would need to be modified to:

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

The query would return all computers with names starting with **DB**. The statement would read *show all computer objects with names beginning with DB*.

If the description of the computer or if the location attribute were also defined in Active Directory, the LDAP query would need to be modified to:

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

The statement would read *show all computer objects with names beginning with DB and with descriptions matching...*

You can also use queries to exclude systems. The **NOT** operator is an exclamation mark (!). To add all DB servers but exclude all systems with **CLUSTER** in their name, the query would need to be modified to:

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

The statement would read *show all computer objects with names beginning with DB but exclude those DB systems with CLUSTER in the name*.

The **OR** operator is the pipe (|) symbol. For example, to add all 2003 and 2008 systems to a **Systems** list:

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

The statement would read, *show all computer objects with operating system 2003 or 2008*. Be careful with queries like this because changing the statement to (&(objectClass=computer)(operatingSystem=*2003*)(operatingSystem=*2008*)) would be interpreted as *show all computers with the operating system 2003 AND 2008*. A system would not have two operating system types listed.

Queries can be more or less complex than what is shown here. Any attribute present in Active Directory may be used for a 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 to exclude all disabled computer accounts, use the following query:

(&(objectCategory=computer)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

The LDAP attributes used are limited to what can be queried for in Active Directory, and the syntax used should be identical.