Contents

Introduction

This document describes why LDAP group queries may not work on an Email Security Appliance (ESA).

Why does the LDAP group query not work with Active Directory?

Why is the LDAP group query not producing the expected results when tested with a user who is definitely a member of the specified group?

With group queries using Microsoft Active Directory, it is necessary to use the distinguished name (DN) of the group rather than it's common name (CN). Below are some examples of what these two items look like:

Common Name (CN):
Administrators
Phoenix-Users

Distinguished Name (DN):
CN=Administrators, DC=Example, DC=Com
CN=Phoenix-Users, OU=Phoenix, DC=Cisco, DC=Com

If you are not sure of what the DN is, you can locate this in Active Directory Users and Computers:

1. Go to the ‘View’ menu and select ‘Advanced Features’
2. From the properties of your desired Group Object, click the ‘Attribute Editor’
3. Scroll to the ‘distinguishedName’ attribute and double click the attribute
4. The full string should be highlighted. Right-click and copy to the clipboard

Once you have the DN of the group, you can use it whenever you specify the name of the group. This includes test queries, content and message filters, and also mail policies.

Another approach would be to use one of the following two programs to find the DN:

ADExplorer:
http://technet.microsoft.com/en-us/sysinternals/bb963907.aspx

Softerra LDAP Browser:
http://www.ldapadministrator.com/download.htm

The general process for using one of these tools for this purpose is outlined below:

1. Connect to your Domain Controller using your LDAP browsing tool

2. Locate a user object who is a member of the group
3. Find the user object's 'memberOf' attribute
4. Find the DN that corresponds to the group you are trying to target
5. Copy the DN of the target group from this attribute