How to use LDAP Accept Query to validate the recipients of inbound messages using Microsoft Active Directory (LDAP)?

Document ID: 118218

Contributed by Dominic Yip and Andreas Mueller, Cisco TAC Engineers.
Aug 12, 2014

Contents

Question:

Question:

How to use LDAP Accept Query to validate the recipients of inbound messages using Microsoft Active Directory (LDAP)?

Note: The following example integrates with a standard Microsoft Active Directory deployment, although the principles can be applied to many types of LDAP implementations.

You will first create an LDAP server entry, at which point you must specify your directory server as well as the query that the Email Security Appliance will perform. The query is then enabled or applied on your incoming (public) listener. These LDAP server settings can be shared by different listeners and other parts of the configuration such as end−user quarantine access.

To facilitate the configuration of the LDAP queries on your IronPort appliance, we recommend that you use an LDAP browser, which allows you to take a look at your schema as well as all the attributes upon which you can query against.

For Microsoft Windows, you can use:

- Softterra's LDAP browser
- Ldp
- Adsiedit

For Linux or UNIX, you can use the `ldapsearch` command.

First, you need to define the LDAP server to query. In this example, the nickname of "PublicLDAP" is given for the *myldapserver.example.com* LDAP server. Queries are directed to TCP port 389 (the default).

NOTE: If your Active Directory implementation contains subdomains, you will not be able to query for users in a sub domain using the base DN of the root domain. However, when using Active Directory, you may also query LDAP against the Global Catalog (GC) Server on TCP port 3268. The GC contains partial information for *all* objects in the Active Directory forest and provides referrals to the subdomain in question when

further information is required. If you cannot "find" users in your subdomains, leave the base DN at the root and set the IronPort to use the GC port.

GUI:

1. Create a new LDAP Server Profile with values located previously from your directory server (System Administration > LDAP). For example:
   - Server Profile Name: *PublicLDAP*
   - Host Name: *myldapserver.example.com*
   - Authentication Method: *Use Password: Enabled*
   - Username:*cn=ESA,cn=Users,dc=example,dc=com*
   - Password: *password*
   - Server Type: *Active Directory*
   - Port: *3268*
   - BaseDN:*dc=example,dc=com*

   Make sure to use the "Test Server(s)" button to verify your settings before continuing. Successful output should look like:

```
Connecting to myldapserver.example.com at port 3268
Bound successfullywithDNCN=ESA,CN=Users,DC=example,DC=com
Result: succeeded
```

2. Use the same screen to define the LDAP accept query. The following example checks the recipient address against the more common attributes, either "mail" OR "proxyAddresses":

   - Name: *PublicLDAP.accept*
   - QueryString:*(|(mail={a})(proxyAddresses=smtp:{a}))*

   You can use the "Test Query" button to verify your search query returns results for a valid account. Successful output searching for the service account's address "esa.admin@example.com" should look like:

```
Query results for host:myldapserver.example.com
Query (mail=esa.admin@example.com) >to server PublicLDAP (myldapserver.example.com:3268)
Query (mail=esa.admin@example.com) lookup success, (myldapserver.example.com:3268) returne
Success: Action: Pass
```

3. Apply this new accept query to the Inbound Listener (Network > Listeners). Expand the options LDAP Queries > Accept, and choose your query PublicLDAP.accept.

4. Finally, commit the changes to enable these settings.

CLI:

1. ***First, you use the ldapconfig command to define an LDAP server for the appliance to bind to, and queries for recipient acceptance (ldapaccept subcommand), routing (ldaprouting subcommand), and masquerading (masquerade subcommand) are configured.***

```
mail3.example.com> ldapconfig
No LDAP server configurations.
Choose the operation you want to perform:
- NEW - Create a new server configuration.
```

```
[]> new
Please create a name for this server configuration (Ex: "PublicLDAP"):
[]> PublicLDAP
Please enter the hostname:
[]> myldapserver.example.com
Use SSL to connect to the LDAP server? [N]> n
Please enter the port number:
[389]> 389
Please enter the base:
[dc=example,dc= com]>dc=example,dc=com
 Select the authentication method to use for this server configuration:
1. Anonymous
2. Password based
[1]> 2
Please enter the bind username:
[cn=Anonymous]>cn=ESA,cn=Users,dc=example,dc=com
Please enter the bind password:
[]> password
Name: PublicLDAP
Hostname: myldapserver.example.com Port 389
Authentication Type: password
Base:dc=example,dc=com
```

2. Second, you need to define the query to perform against the LDAP server you have just configured.

```
Choose the operation you want to perform:
- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or bounced/dropped
- LDAPROUTING - Configure message routing.    - MASQUERADE - Configure domain masquerading
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
[]> ldapaccept
Please create a name for this query:
[PublicLDAP.ldapaccept]> PublicLDAP.ldapaccept
Enter the LDAP query string:
[(mailLocalAddress= {a})]>(|(mail={a})(proxyAddresses=smtp:{a}))
Please enter the cache TTL in seconds:
[900]>
 Please enter the maximum number of cache entries to retain:
[10000]>
Do you want to test this query? [Y]> n
Name: PublicLDAP
Hostname: myldapserver.example.com Port 389
Authentication Type: password
Base:dc=example,dc=com
LDAPACCEPT: PublicLDAP.ldapaccept
```

3. Once you have configured the LDAP query, you need to apply the LDAPaccept policy to your Inbound Listener.

```
example.com> listenerconfig
Currently configured listeners:
1. Inboundmail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. Outboundmail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit
Enter the name or number of the listener you wish to edit.
[]> 1
```

```
Name: InboundMail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: Off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS >- Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
- LDAPACCEPT - Configure an LDAP query to determine whether a recipient address should be
accepted or bounced/dropped.
- LDAPROUTING - Configure an LDAP query to reroute messages.
[]> ldapaccept    Available Recipient Acceptance Queries
1. None
2. PublicLDAP.ldapaccept
[1]> 2
Should the recipient acceptance query drop recipients or bounce them?
NOTE: Directory Harvest Attack Prevention may cause recipients to be
dropped regardless of this setting.
1. bounce
2. drop
[2]> 2
Name: InboundMail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: ldapaccept (PublicLDAP.ldapaccept)
```

4. To activate the changes made to the listener, commit your changes.