使用Microsoft Active Directory (LDAP)，如何使用LDAP接受查询验证入站消息的收件人？

目录

问题：

使用Microsoft Active Directory (LDAP)，如何使用LDAP接受查询验证入站消息的收件人？

注意：以下示例集成一标准的Microsoft Active Directory部署，虽然原理可以应用到LDAP实施的许多类型。

您首先将创建LDAP服务器条目，到时您必须指定电子邮件安全工具将执行的您的目录服务器以及查询。 查询在您的流入(公共)监听程序然后启用或应用。这些LDAP服务器设置可以由不同的监听程序和配置的其他部分共享例如最终用户检疫访问。

要实现LDAP查询的配置在您的IronPort设备的，我们建议您使用一个LDAP浏览器，允许您采取查看在您的模式以及所有属性您能查询。

对于Microsoft Windows，您能使用：

对于Linux或UNIX，您能使用`ldapsearch`命令。

首先，您需要定义LDAP服务器查询。在本例中，“PublicLDAP”昵称为*myldapserver.example.com* LDAP服务器给。查询处理对TCP端口389 (默认)。

注意：如果您的活动目录实施包含子域，使用根域的基础DN，您不能查询一个子域的用户。然而，当曾经活动目录时，您可以也查询LDAP在TCP端口3268的Global Catalog (GC)服务器。当更多信息要求时， GC在活动目录森林里包含*all*对象的部分信息并且提供推举给有问题的子域。如果“找不到”您的子域的用户，请留下基础DN在根并且设置IronPort使用GC端口。

GUI ：

1. 创建与从您的目录服务器以前查找的值的一新的LDAP服务器配置文件(系统管理> LDAP)。 例如： 服务器配置文件名称：*PublicLDAP*主机名：*myldapserver.example.com*认证方法：*使用密码：已启用*用户名：*cn=ESA， cn=users， dc=example， dc=com*密码：*密码*服务器类型:*Active Directory*波尔特：*3268*BaseDN ：*dc=example， dc=com*确保使用“测验服务器”按钮

在继续前验证您的设置。 成功的输出应该看似类似：

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

2. 请使用同样屏幕定义LDAP接受查询。 以下示例根据更加普通的属性检查接收地址，“邮件”或“proxyAddresses”：名称：*PublicLDAP.accept*QueryString ： *(|(mail= {a}) (proxyAddresses=smtp ：{a}))*您能使用“测验查询”按钮验证您的一个有效帐户的搜索查询回归结果。 搜索服务帐户的地址“esa.admin@example.com”的成功的输出应该看似类似：

```
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) returned
1 results
Success: Action: Pass
```

3. 应用新的此接受查询给入站监听程序(网络>监听程序)。 展开选项LDAP查询>接受，并且选择您的查询PublicLDAP.accept。

4. 最后，请确认更改启用这些设置。

CLI ：

1. **首先，您使用*ldapconfig*命令定义设备的一个LDAP服务器能绑定对，并且接收接受的(ldapaccept子命令)化妆的查询，路由(ldaprouting的子命令)和(化妆舞会子命令)配置。**

```
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. 其次，您需要定义查询实行您配置的LDAP服务器。

```
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. 一旦配置LDAP查询，您需要运用LDAPaccept策略对您的入站监听程序。

```
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. 要激活做的变动对监听程序，请确认您的更改。