如何使用LDAP接受查詢驗證使用Microsoft Active Directory(LDAP)的入站郵件的收件人？

目錄

問題：

如何使用LDAP接受查詢驗證使用Microsoft Active Directory(LDAP)的入站郵件的收件人？

附註：以下示例與標準Microsoft Active Directory部署整合，不過這些原則可以應用於許多型別的LDAP實施。

您將首先建立LDAP伺服器條目，此時必須指定目錄伺服器以及郵件安全裝置將執行的查詢。 然後，在傳入（公共）監聽器上啟用或應用查詢。這些LDAP伺服器設定可以由不同的偵聽程式以及配置的其他部分（如終端使用者隔離訪問）共用。

為了便於在IronPort裝置上配置LDAP查詢，我們建議您使用LDAP瀏覽器，這樣您就可以檢視自己的架構以及可以查詢所依據的所有屬性。

對於Microsoft Windows，可以使用：

對於Linux或UNIX，可以使用 `ldapsearch` 指令。

首先，您需要定義要查詢的LDAP伺服器。在本示例中，為*myldapserver.example.com* LDAP伺服器指定了「PublicLDAP」的別名。查詢定向到TCP埠389（預設值）。

附註：如果Active Directory實現包含子域，您將無法使用根域的基本DN查詢子域中的使用者。但是，使用Active Directory時，您還可以根據TCP埠3268上的全域性目錄(GC)伺服器查詢LDAP。GC包含Active Directory林中*all*對象的部分資訊，並在需要更多資訊時提供對所討論子域的引用。如果您在子域中無法「查詢」使用者，請將基本DN留在根位置，並將IronPort設定為使用GC埠。

GUI:

1. 使用先前位於目錄伺服器（系統管理> LDAP）中的值建立新的LDAP伺服器配置檔案。 例如：伺服器配置檔名稱：*PublicLDAP*主機名：*myldapserver.example.com*身份驗證方法：*使用密碼：已啟用*使用者名稱:*cn=ESA，cn=Users，dc=example，dc=com*密碼：*密碼*伺服器型別：*Active Directory*連接埠:*3268*BaseDN:*dc=example，dc=com*繼續之前，請確保使用「測試

伺服器」按鈕驗證您的設定。 成功的輸出應如下所示：

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

2. 使用同一螢幕定義LDAP接受查詢。 以下示例根據更常見屬性（即「mail」或「proxyAddresses」）檢查收件人地址：名稱:*PublicLDAP.accept*QueryString:*(|(mail={a})(proxyAddresses=smtp:{a}))*您可以使用「測試查詢」按鈕來驗證搜尋查詢是否返回有效帳戶的結果。 搜尋服務帳戶地址「esa.admin@example.com」的成功輸出應如下所示：

```
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. 將此新的accept查詢應用於入站監聽程式（「網路」>「監聽程式」）。 展開選項LDAP Queries > Accept，然後選擇您的查詢PublicLDAP.accept。

4. 最後，提交更改以啟用這些設定。

CLI:

1. **首先，使用*ldapconfig*命令為要繫結的裝置定義LDAP伺服器，並配置收件人接受（ldapaccept子命令）、路由（ldaprouting子命令）和偽裝（偽裝子命令）查詢。**

```
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，您需要定義要針對剛配置的LDAP伺服器執行的查詢。

```
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. 配置LDAP查詢後，需要將LDAP接受策略應用到入站監聽程式。

```
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. 要啟用對監聽程式所做的更改，請提交更改。