LDAP 受け入れクエリーを使用して、Microsoft Active Directory（LDAP）を使用した着信メッセージの受信者を確認するにはどうすればよいですか。

目次

質問：

LDAP 受け入れクエリーを使用して、Microsoft Active Directory（LDAP）を使用した着信メッセージの受信者を確認するにはどうすればよいですか。

注： 次の例は標準の Microsoft Active Directory 展開に関連するものですが、この原則は多くの種類の LDAP 実装に適用できます。

最初に LDAP サーバ エントリを作成し、そこでディレクトリ サーバと、E メール セキュリティ アプライアンスが実行するクエリーを指定する必要があります。 このクエリーは、着信（パブリック）リスナーで有効にされるか、または適用されます。 これらの LDAP サーバ設定は、異なるリスナー、およびエンドユーザ保証アクセスなどの設定の他の部分によって共有できます。

IronPort アプライアンスでの LDAP クエリーの設定を簡単にするために、LDAP ブラウザを使用することをお勧めします。LDAP ブラウザでは、クエリー対象のすべての属性に加えてスキーマを参照できます。

Microsoft Windows の場合、次のものを使用できます。

Linux または UNIX の場合、ldapsearch コマンドを使用できます。

最初に、クエリーを実行するための LDAP サーバを定義する必要があります。 この例では、*myldapserver.example.com* LDAP サーバに対して「PublicLDAP」というニックネームが付けられています。 クエリーの送信先は、TCP ポート 389（デフォルト値）です。

注： Active Directory の実装にサブドメインが含まれている場合、ルート ドメインのベース DN を使用してサブドメインのユーザに関するクエリーを実行できません。 ただし、Active Directory を使用する場合、TCP ポート 3268 でグローバル カタログ（GC）サーバに対して LDAP クエリーを実行することもできます。 GC サーバには Active Directory フォレストのすべてのオブジェクトに関する一部の情報が含まれており、詳細な情報が必要なときには対象サブドメインへの参

照を示します。 サブドメインにユーザが見つからない場合、ベース DN をルートのままにし、GC ポートを使用するように IronPort を設定します。

GUI：

1. ディレクトリ サーバの既存の値を使用して新しい LDAP サーバ プロファイルを作成します（[System Administration] > [LDAP]）。 次に、例を示します。 Server Profile Name：*PublicLDAP*Host Name： *myldapserver.example.com*[Authentication Method]： *Use Password: Enabled*ユーザ名： *cn=ESA,cn=Users,dc=example,dc=com*パスワード：*password*Server Type： *Active Directory*Port: *3268*BaseDN： *dc=example,dc=com*[Test Server(s)] ボタンを使用して設定を検証してから続行します。 正常な出力は次のようになります。

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

2. 同じ画面を使用して LDAP 受け入れクエリーを定義します。 次の例では、より一般的な属性である「mail」または「proxyAddresses」と照らし合わせて受信者アドレスをチェックします。[Name]： *PublicLDAP.accept*QueryString： *(((|((mail={a})(proxyAddresses=smtp:{{a}))*[Test Query] ボタンを使用して、検索クエリーが有効のアカウントを返すことを検証します。 サービス アカウントのアドレス「esa.admin@example.com」の検索の正常な出力は次のようになります。

```
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. この新しい受け入れクエリーをインバウンド リスナー（[Network] > [Listeners]）に適用します。 オプション [Queries] > [Accept] を展開し、PublicLDAP.accept クエリーを選択します。

4. 最後に、変更をコミットしてこれらの設定を有効にします。

CLI：

1. **最初に、*ldapconfig* コマンドを使用して、アプライアンスのバインド先となる LDAP サーバを定義し、受信者受け入れ（ldapaccept サブコマンド）、ルーティング（ldaprouting サブコマンド）、およびマスカレード（masquerade サブコマンド）のクエリーをを設定します。**

```
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. 次に、設定した LDAP サーバに対して実行するクエリーを定義する必要があります。

```
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. LDAP クエリーを設定したら、インバウンド リスナーに LDAPaccept ポリシーを適用する必要があります。

```
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. リスナーに対して加えた変更を有効にするには、変更をコミットします。