

目次

[質問：](#)

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：

PublicLDAPHost 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。

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.acceptQueryString : (((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。
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。
。
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。
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。
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。