LDAP クエリ

この章は、次の項で構成されています。

LDAP クエリの概要

クラウドEメールセキュリティアプライアンスのLDAP設定は変更しないことを推奨します。

ユーザ情報がネットワーク インフラストラクチャ内の LDAP ディレクトリ（Microsoft Active Directory、SunONE Directory Server、OpenLDAP などのディレクトリ）に格納されている場合は、メッセージの受け入れ、ルーティング、および認証のためにLDAPサーバに対してクエリを実行するようにアプライアンスを設定できます。アプライアンスは、1つまたは複数のLDAPサーバと連携させるように設定できます。

ここでは、実行できる LDAP クエリのタイプと、LDAP とアプライアンスとが連携してメッセージの認証、受け入れ、ルーティングを行うし仕組み、およびLDAPと連携するようにアプライアンスを設定する方法について概説します。

関連項目

- LDAP クエリについて （2 ページ）
- LDAP と AsyncOS との連携の仕組み （3 ページ）
- Cisco IronPort アプライアンスを LDAP サーバと連携させるための設定 （4 ページ）
- LDAP サーバに関する情報を格納する LDAP サーバ プロファイルの作成 （5 ページ）
- LDAP サーバのテスト （7 ページ）
- 特定のリスナーで実行する LDAP クエリの有効化 （8 ページ）
- Microsoft Exchange 5.5 に対する拡張サポート （11 ページ）

LDAP クエリについて

ユーザ情報がネットワーク インフラストラクチャ内の LDAP ディレクトリに格納されている場合は、次の目的でLDAPサーバに対してクエリを実行するようにアプライアンスを設定できます。

- **受け入れクエリ**。既存のLDAPインフラストラクチャを使用して、着信メッセージ（パブリック リスナーでの）の受信者メール アドレスの扱い方を定義できます。詳細については、受信者検証で受け入れクエリを使用する （21 ページ）を参照してください。
- **ルーティング（エイリアシング）**。ネットワーク内のLDAPディレクトリに格納されている情報に基づいてメッセージを適切なアドレスやメール ホストへルーティングするように、アプライアンスを設定できます。詳細については、複数ターゲットアドレスへのメール送信にルーティング クエリを使用する （23 ページ）を参照してください。
- **証明書認証**。ユーザのメール クライアントと E メール セキュリティ アプライアンス間の SMTP セッションを認証するためのクライアント証明書の有効性を確認するクエリを作成できます。詳細については、クライアント証明書の有効性の確認を参照してください。
- **マスカレード**。発信メールの場合はエンベロープ送信者、着信メールの場合はメッセージ ヘッダー（To:、Reply To:、From:、CC:など）をマスカレードできます。マスカレードの詳細については、エンベロープ送信者を書き換えるためのマスカレード クエリの使用 （24 ページ）を参照してください。
- **グループ クエリ**。LDAP ディレクトリ内のグループに基づいてメッセージに対するアクションを実行するようにアプライアンスを設定できます。このように設定するには、グループ クエリとメッセージ フィルタとを関連付けます。定義済みの LDAP グループに一致するメッセージに対しては、メッセージ フィルタに使用できる任意のメッセージ アクションを実行できます。詳細については、受信者がグループ メンバーであるかどうかを判別するグループ LDAP クエリの使用 （26 ページ）を参照してください。
- **ドメインベース クエリ**。ドメインベース クエリを作成すると、アプライアンスは同じリスナー上でドメインごとに異なるクエリを実行できます。E メール セキュリティ アプライアンスがドメインベース クエリを実行するときは、どのクエリを使用するかをドメインに基づいて決定し、そのドメインに関連付けられているLDAPサーバに対してクエリを実行します。

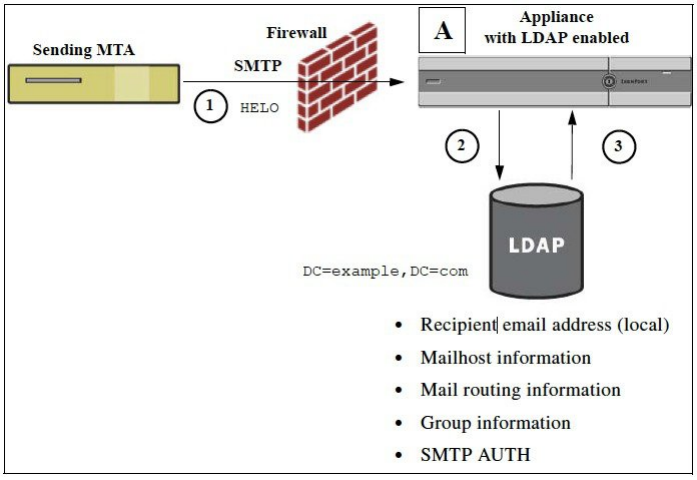
- **チェーン クエリ。**チェーン クエリを作成すると、アプライアンスに一連のクエリを順番に実行させることができます。チェーン クエリが設定済みのときは、アプライアンスはシーケンス内のクエリを 1 つずつ実行し、LDAP アプライアンスから肯定的な結果が返されると実行を停止します。チェーン ルーティング クエリーでは、アプライアンスは書き換えられた電子メール アドレスごとに、同じ設定の一連のチェーン クエリーを再実行します。
- **ディレクトリ ハーベスト防止。**LDAP ディレクトリを使用したディレクトリ ハーベスト攻撃を防ぐようにアプライアンスを設定できます。ディレクトリ ハーベスト防止は、SMTP カンバセーション中に行うことも、ワーク キューの中で行うこともできます。受信者が LDAP ディレクトリ内で見つからない場合に、遅延バウンスを実行するか、そのメッセージ全体をドロップするかを設定できます。その結果、スパム送信者はメールアドレスが有効なものかどうかを区別できなくなります。LDAP によるディレクトリ ハーベスト攻撃防止 （34 ページ）を参照してください。
- **SMTP 認証。**AsyncOS では、SMTP 認証がサポートされています。SMTP Auth は、SMTP サーバに接続するクライアントを認証するメカニズムです。この機能を利用すると、ユーザはリモート接続するとき（たとえば自宅や出張先にいる場合）でも、メール サーバを使用してメールを送信できるようになります。詳細については、SMTP 認証を行うための AsyncOS の設定 （37 ページ）を参照してください。
- **外部認証。**アプライアンスにログインするユーザの認証を LDAP ディレクトリを使用して行うようにアプライアンスを設定できます。詳細については、ユーザの外部 LDAP 認証の設定 （46 ページ）を参照してください。
- **スパム検疫エンドユーザ認証。**エンドユーザ隔離画面にログインするユーザを検証するように、アプライアンスを設定できます。詳細については、スパム隔離機能へのエンドユーザ認証 （49 ページ）を参照してください。
- **スパム検疫エイリアス統合。**スパムに関する電子メール通知を使用する場合、このクエリを使用してエンドユーザのエイリアスを統合すると、エンドユーザがエイリアスのメールアドレスごとに隔離通知を受け取ることはなくなります。詳細については、スパム隔離のエイリアス統合クエリ （51 ページ）を参照してください。

LDAP と AsyncOS との連携の仕組み

LDAP ディレクトリとプライアンスとを連携させると、受信者受け入れ、メッセージルーティング、およびヘッダー マスカレードに LDAP ディレクトリ サーバを使用できます。LDAP グループ クエリをメッセージ フィルタと併用すると、メッセージがアプライアンスで受信されたときの取り扱いのルールを作成できます。

次の図は、アプライアンスが LDAP とどのように連携するかを示しています。

図 *1 : LDAP* 設定



1. 送信側 MTA からパブリック リスナー「A」に SMTP 経由でメッセージが送信されます。
2. アプライアンスは、LDAP サーバに対してクエリを実行します。この LDAP サーバは [システム管理（System Administration）] > [LDAP] ページ（またはグローバル **ldapconfig** コマンド）で定義されます。
3. データが LDAP ディレクトリから受信されます。リスナーで使用するように [システム管理（System Administration）] > [LDAP] ページ（または **ldapconfig** コマンド）で定義されたクエリに応じて、次の処理が実行されます。
   - メッセージを新しい受信者アドレスにルーティングするか、ドロップまたはバウンスする
   - メッセージを新しい受信者のメールホストにルーティングする
   - メッセージ ヘッダー From:、To:、CC: をクエリに基づいて書き換える
   - メッセージ フィルタ ルール **rcpt-to-group** または **mail-from-group** で定義された、それ以降のアクション（グループ クエリと組み合わせて使用）。

（注） 複数の LDAP サーバに接続するようにアプライアンスを設定できます。その場合、複数の LDAP サーバを使用して、ロード バランシングやフェールオーバーを行うように LDAP プロファイルを設定できます。複数の LDAP サーバと連携させる方法の詳細については、AsyncOS を複数の LDAP サーバと連携させるための設定 （53 ページ）を参照してください。

Cisco IronPort アプライアンスを LDAP サーバと連携させるための設定

受け入れ、ルーティング、エイリアシング、およびマスカレードのためにアプライアンスを LDAP ディレクトリと連携させるには、以下の手順に従って AsyncOS アプライアンスを設定する必要があります。

手順

ステップ 1 **LDAP サーバ プロファイルを設定します。**サーバ プロファイルに、AsyncOS から LDAP サーバに接続するための次の情報を設定します。

- クエリ送信先となるサーバの名前とポート
- ベース DN
- サーバとのバインドのための認証要件

サーバプロファイルの設定方法の詳細については、LDAPサーバに関する情報を格納するLDAPサーバ プロファイルの作成 （5 ページ） を参照してください。

LDAP サーバ プロファイルを設定するときに、AsyncOS からの接続先となる LDAP サーバを 1 つまたは複数設定できます。

AsyncOSから複数のサーバに接続するように設定する方法については、AsyncOSを複数のLDAPサーバと連携させるための設定 （53 ページ）を参照してください。

ステップ 2 **LDAP クエリを設定します。**LDAP クエリは、LDAP サーバ プロファイルで設定します。ここで設定するクエリは、実際に使用するLDAPの実装とスキーマに合わせて調整してください。

作成できる LDAP クエリのタイプについては、LDAP クエリについて （2 ページ）を参照してください。

クエリの記述方法については、LDAPクエリに関する作業 （13ページ）を参照してください。

ステップ 3 **LDAPサーバプロファイルをパブリック リスナーまたはプライベート リスナーに対してイネーブルにします。**LDAPサーバプロファイルをリスナーに対してイネーブルにすると、そのリスナーによって、メッセージの受け入れ、ルーティング、または送信の際にLDAPクエリが実行されるようになります。

詳細については、特定のリスナーで実行する LDAP クエリの有効化 （8 ページ）を参照してください。

（注） グループ クエリを設定するときは、AsyncOS と LDAP サーバとを連携させるためにさらに設定作業が必要です。グループ クエリの設定方法については、受信者がグループ メンバーであるかどうかを判別するグループ LDAP クエリの使用 （26 ページ）を参照してください。エンドユーザ認証またはスパム通知統合のクエリを設定するときは、スパム隔離機能への LDAP エンドユーザ アクセスをイネーブルにする必要があります。スパム隔離の詳細については、「スパム隔離」の章を参照してください。

LDAPサーバに関する情報を格納するLDAPサーバプロファイルの作成

LDAPディレクトリを使用するようにAsyncOSを設定するには、LDAPサーバに関する情報を格納する LDAP サーバ プロファイルを作成します。

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] ページの [LDAPサーバプロファイルを追加（Add LDAP Server Profile）] をクリックします。

ステップ 2 サーバ プロファイルの名前を入力します。

ステップ 3 LDAP サーバのホスト名を入力します。

複数のホスト名を入力すると、LDAP サーバのフェールオーバーやロードバランシングができるようになります。複数のエントリを指定する場合は、カンマで区切ります。詳細については、AsyncOS を複数の LDAP サーバと連携させるための設定 （53 ページ）を参照してください。

ステップ 4 認証方法を選択します。匿名認証を使用することも、ユーザ名とパスフレーズを指定することもできます。

ステップ 5 LDAP サーバのタイプを、[Active Directory]、[OpenLDAP]、[不明またはそれ以外（Unknown or Other）] から選択します。

ステップ 6 ポート番号を入力します。

Active Directory または不明/その他のサーバ タイプの場合、デフォルトのポートは、SSL なしが 3268、SSL ありが 3269 です。

Open LDAP サーバ タイプの場合、デフォルトのポートは、SSL なしが 389、SSL ありが 636 です。

ステップ 7 LDAP サーバのベース DN（識別名）を入力します。

ユーザ名とパスフレーズを使用して認証する場合は、パスフレーズが格納されているエントリへの完全DNがユーザ名に含まれている必要があります。たとえば、マーケティング グループに属しているユーザの電子メール アドレスが joe@example.com であるとします。このユーザのエントリは、次のようになります。

```
uid=joe, ou=marketing, dc=example dc=com
```

ステップ 8 LDAP サーバとの通信に SSL を使用するかどうかを選択します。

ステップ 9 [詳細（Advanced）] で、キャッシュの存続可能時間を入力します。この値は、キャッシュを保持する時間の長さです。

ステップ 10 保持するキャッシュ エントリの最大数を入力します。

（注） このキャッシュは、LDAP サーバごとに保持されます。複数の LDAP サーバを設定する場合は、パフォーマンスを向上させるために、LDAP キャッシュの値を小さく設定する必要があります。また、アプライアンスでのさまざまなプロセスのメモリ使用率が高い場合、この値を大きくすると、システムのパフォーマンスが低下する可能性があります。

ステップ 11 同時接続の数を入力します。

- ロード バランシングのために LDAP サーバ プロファイルを設定する場合、これらの接続はリストで指定された LDAP サーバ間で配分されます。たとえば、同時接続数を 10 と設

定し、3 台のサーバを使用して接続のロードバランシングを行う場合は、AsyncOS によってサーバへの接続が 10 ずつ作成され、接続の総数は 30 となります。

（注） 同時接続の最大数には、LDAP クエリーに使用される LDAP 接続も含まれます。ただし、スパム隔離機能に対して LDAP 認証を使用する場合は、これよりも多くの接続が開かれることがあります。

- 接続がリセットされる前に LDAP サーバへの接続を維持する必要がある最大時間（秒単位）を設定できます。60 ～ 86400 の間の値を選択します。

ステップ 12 サーバへの接続をテストするために、[テストサーバ（Test Server(s)）] ボタンをクリックします。複数の LDAP サーバを指定した場合は、すべてのサーバのテストが実行されます。テストの結果が [接続ステータス（Connection Status）] フィールドに表示されます。詳細については、LDAP サーバのテスト （7 ページ）を参照してください。

ステップ 13 クエリを作成します。該当するチェックボックスをオンにして、フィールドに入力します。選択できるのは、[承認（Accept）]、[ルーティング（Routing）]、[マスカレード（Masquerade）]、[グループ（Group）]、[SMTP認証（SMTP Authentication）]、[外部認証（External Authentication）]、[スパム隔離エンドユーザ認証（Spam Quarantine End-User Authentication）]、[スパム隔離エイリアス統合（Spam Quarantine Alias Consolidation）] です。

（注） メッセージを受信または送信するときにアプライアンスが LDAP クエリを実行できるようにするには、該当するリスナーに対して LDAP クエリをイネーブルにする必要があります。詳細については、特定のリスナーで実行する LDAP クエリの有効化 （8 ページ）を参照してください。

ステップ 14 クエリをテストするために、[クエリのテスト（Test Query）] ボタンをクリックします。

テスト パラメータを入力して [テストの実行（Run Test）] をクリックします。テストの結果が [接続ステータス（Connection Status）] フィールドに表示されます。クエリーの定義や属性に変更を加えた場合は、[更新（Update）] をクリックします。詳細については、LDAP サーバのテスト （7 ページ）を参照してください。

（注） 空パスフレーズでのバインドを許可するように LDAP サーバが設定されている場合は、パスフレーズ フィールドが空でもクエリのテストは合格となります。

ステップ 15 変更を送信し、保存します。

（注） サーバ設定の数に制限はありませんが、設定できるクエリは、サーバ 1 台につき受信者受け入れ 1 つ、ルーティング 1 つ、マスカレード 1 つ、グループ クエリ 1 つのみです。

LDAP サーバのテスト

[LDAP サーバプロファイルの追加/編集（Add/Edit LDAP Server Profile）] ページの [テストサーバ（Test Server(s)）] ボタン（または CLI の ldapconfig コマンドの test サブコマンド）を使用し

て、LDAP サーバへの接続をテストします。サーバ ポートへの接続に成功したか失敗したかを示すメッセージが表示されます。複数の LDAP サーバが設定されている場合は、各サーバのテストが実行されて、結果が個別に表示されます。

特定のリスナーで実行する LDAP クエリの有効化

メッセージを受信または送信するときにアプライアンスが LDAP クエリを実行できるようにするには、該当するリスナーに対して LDAP クエリをイネーブルにする必要があります。

関連項目

- LDAP クエリのグローバル設定の構成 （8 ページ）
- LDAP サーバ プロファイル作成の例 （8 ページ）
- パブリック リスナー上の LDAP クエリの有効化 （10 ページ）
- プライベート リスナーでの LDAP クエリのイネーブル化 （10 ページ）

LDAP クエリのグローバル設定の構成

LDAP グローバル設定では、すべての LDAP トラフィックをアプライアンスがどのように扱うかを定義します。

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] ページの [設定を編集（Edit Settings）] をクリックします。

ステップ 2 LDAP トラフィックに使用する IP インターフェイスを選択します。インターフェイスの 1 つが自動的にデフォルトとして選択されます。

ステップ 3 LDAP インターフェイスに使用する TLS 証明書を選択します（[ネットワーク（Network）] > [証明書（Certificates）] ページまたは CLI の **certconfig** コマンドを使用して追加された TLS 証明書。他の MTA との暗号化通信の概要を参照してください）。

ステップ 4 LDAP サーバ証明書を検証する場合は、適切なオプションを選択します。

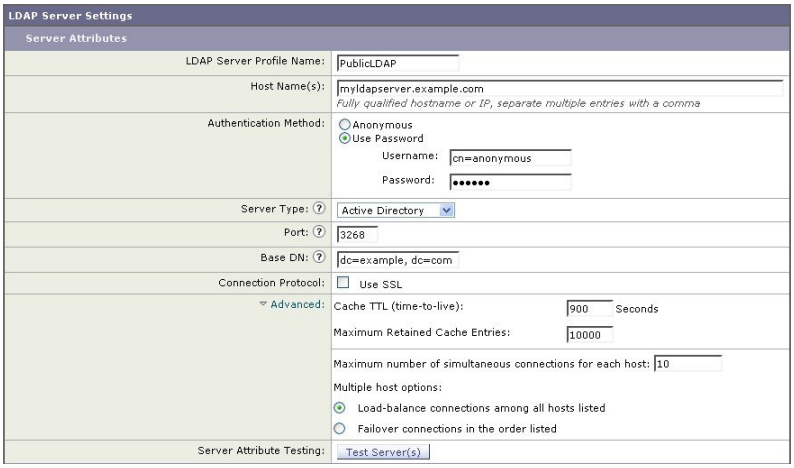
ステップ 5 変更を送信し、保存します。

LDAP サーバ プロファイル作成の例

次に示す例では、[システム管理（System Administration）] > [LDAP] ページ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、ルーティング、およびマスカレードのクエリを設定します。

（注） LDAP 接続試行のタイムアウトは 60 秒です。この時間には、DNS ルックアップと接続そのものに加えて、アプライアンス自体の認証バインド（該当する場合）も含まれます。初回の失敗後は、同じサーバ内の別のホストに対する試行がただちに行われます（2 つ以上のホストをカンマ区切りリストで指定した場合）。サーバ内にホストが 1 つしかない場合は、そのホストへの接続が繰り返し試行されます。

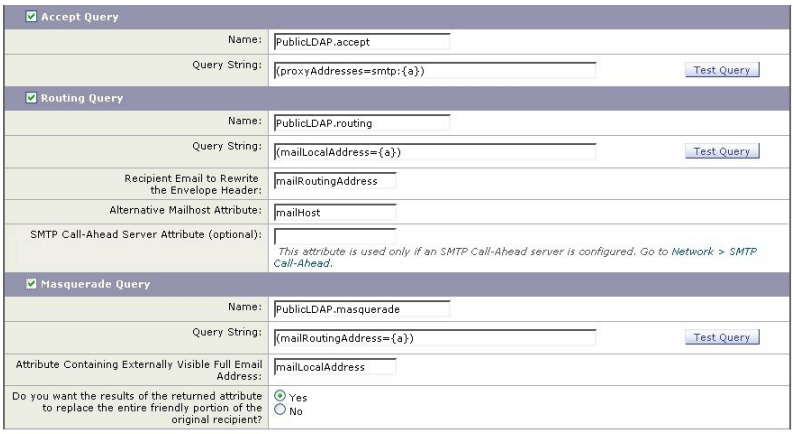
図 *2 : LDAP* サーバ プロファイルの設定（*1/2*）



初めに、「PublicLDAP」というニックネームを myldapserver.example.com LDAP サーバに与えます。接続数は 10（デフォルト値）に設定されており、複数 LDAP サーバ（ホスト）のロード バランス オプションはデフォルトのままとなっています。ここで複数のホストの名前を、カンマ区切りのリストとして指定できます。クエリの送信先は、ポート 3268（デフォルト値）です。SSL は、このホストの接続プロトコルとしてはイネーブルになっていません。example.com のベース DN が定義されています（dc=example,dc=com）。キャッシュの存続可能時間は 900 秒、キャッシュ エントリの最大数は 10000 に設定されています。認証方式は、パスフレーズ認証に設定されています。

受信者受け入れ、メール ルーティング、およびマスカレードのクエリが定義されています。クエリー名では、大文字と小文字が区別されます。正しい結果が返されるようにするには、正確に一致している必要があります。

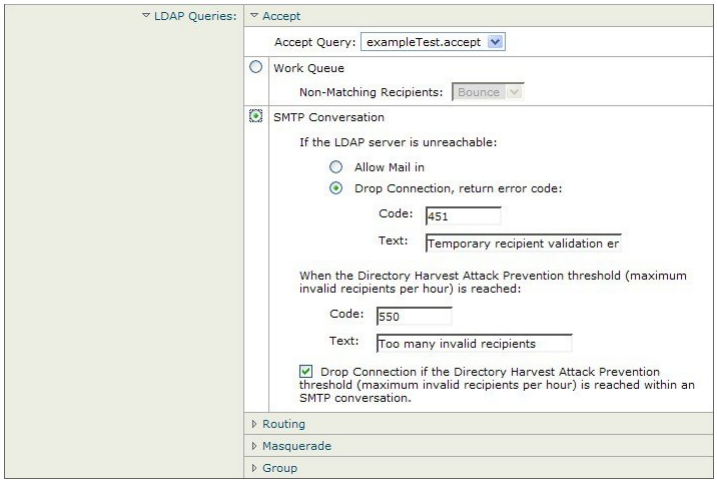
図 *3 : LDAP* サーバ プロファイルの設定（*2/2*）



パブリック リスナー上の LDAP クエリの有効化

この例では、受信者受け入れに対して LDAP クエリを使用するように、パブリック リスナー「InboundMail」を更新します。さらに、受信者受け入れの判定を SMTP カンバセーション中に行うように設定します（詳細については、受信者検証で受け入れクエリを使用する （21 ページ）を参照してください）。

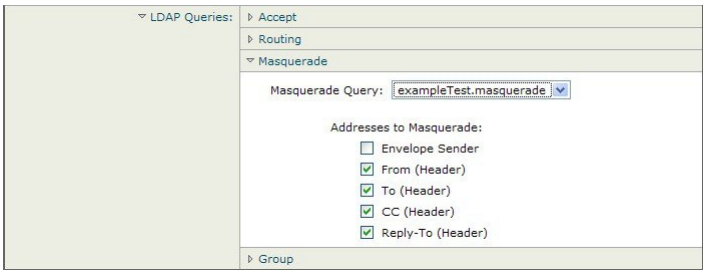
図 *4 :* リスナーでの受け入れとルーティングのクエリのイネーブル化



プライベート リスナーでの LDAP クエリのイネーブル化

この例では、LDAP クエリを使用してマスカレードを行うように、プライベート リスナー「OutboundMail」を更新します。マスカレード対象のフィールドには、From、To、CC、Reply-To があります。

図 *5:* リスナーでのマスカレード クエリのイネーブル化



Microsoft Exchange 5.5 に対する拡張サポート

AsyncOS には、Microsoft Exchange 5.5 をサポートするための設定オプションがあります。これよりも新しいバージョンの Microsoft Exchange を使用する場合は、このオプションをイネーブルにする必要はありません。LDAP サーバを設定するときに、Microsoft Exchange 5.5 サポートをイネーブルにするかどうかを選択できます。選択するには、CLI を使用する必要があります。次に示すように、`ldapconfig -> edit -> server -> compatibility` サブコマンドを実行して、質問に「y」と答えます。

```
mail3.example.com> ldapconfig

Current LDAP server configurations:

1. PublicLDAP: (ldapexample.com:389)


Choose the operation you want to perform:

- NEW - Create a new server configuration.

- EDIT - Modify a server configuration.

- DELETE - Remove a server configuration.


[]> edit

Enter the name or number of the server configuration you wish to edit.

[]> 1

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com

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.

[]> server

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com


Microsoft Exchange 5.5 Compatibility Mode: Disabled

Choose the operation you want to perform:

- NAME - Change the name of this configuration.

- HOSTNAME - Change the hostname used for this query.

- PORT - Configure the port.

- AUTHTYPE - Choose the authentication type.

- BASE - Configure the query base.

- COMPATIBILITY - Set LDAP protocol compatibility options.

[]> compatibility
Would you like to enable Microsoft Exchange 5.5 LDAP compatibility mode? (This is not
recommended for versions of Microsoft Exchange later than 5.5, or other LDAP servers.)


[N]> y

Do you want to configure advanced LDAP compatibility settings? (Typically not required)

[N]>

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com

Microsoft Exchange 5.5 Compatibility Mode: Enabled (attribute "objectClass")

Choose the operation you want to perform:

- NAME - Change the name of this configuration.

- HOSTNAME - Change the hostname used for this query.

- PORT - Configure the port.
```

```
- AUTHTYPE - Choose the authentication type.

- BASE - Configure the query base.

- COMPATIBILITY - Set LDAP protocol compatibility options.

[]>
```

LDAP クエリに関する作業

LDAP サーバ プロファイル内に、実行したい LDAP クエリのタイプごとに 1 つのエントリを作成します。LDAP クエリを作成するときは、実際に使用する LDAP サーバのクエリ構文で入力する必要があります。作成するクエリーは、実際に使用する LDAP ディレクトリ サービスの実装に合わせて調整が必要であることに注意してください。特に、組織固有のニーズを満たすように新しいオブジェクト クラスや属性がディレクトリに追加されている場合です。

関連項目

- LDAP クエリのタイプ （13 ページ）
- ベース識別名（DN） （14 ページ）
- LDAP クエリの構文 （14 ページ）
- セキュア LDAP（SSL） （15 ページ）
- ルーティング クエリー （15 ページ）
- LDAP サーバへの匿名のバインドをクライアントに許可する （15 ページ）
- LDAP クエリのテスト （19 ページ）
- LDAP サーバへの接続のトラブルシューティング （21 ページ）

LDAP クエリのタイプ

- **受け入れクエリ**。詳細については、受信者検証で受け入れクエリを使用する （21 ページ）を参照してください。
- **ルーティング クエリ**。詳細については、複数ターゲット アドレスへのメール送信にルーティング クエリを使用する （23 ページ）を参照してください。
- **証明書認証クエリ**。詳細については、クライアント証明書の有効性の確認を参照してください。
- **マスカレード クエリ**。詳細については、エンベロープ送信者を書き換えるためのマスカレード クエリの使用 （24 ページ）を参照してください。
- **グループ クエリ**。詳細については、受信者がグループ メンバーであるかどうかを判別するグループ LDAP クエリの使用 （26 ページ）を参照してください。
- **ドメインベース クエリ**。詳細については、特定のドメインへルーティングするためのドメイン ベース クエリの使用 （30 ページ）を参照してください。
- **チェーン クエリ**。詳細については、一連の LDAP クエリを実行するためのチェーン クエリの使用 （32 ページ）を参照してください。

次の目的のためにクエリを設定することもできます。

- **ディレクトリ ハーベスト防止**。詳細については、LDAP クエリについて （2 ページ）を参照してください。
- **SMTP 認証**。詳細については、SMTP 認証を行うための AsyncOS の設定 （37 ページ）を参照してください。
- 外部認証。 詳細については、ユーザの外部 LDAP 認証の設定 （46 ページ）を参照してください。
- **スパム隔離エンドユーザ認証クエリー**。詳細については、スパム隔離機能へのエンドユーザ認証 （49 ページ）を参照してください。
- **スパム隔離エイリアス統合クエリー**。詳細については、スパム隔離のエイリアス統合クエリ （51 ページ）を参照してください。

指定した検索クエリは、システム上で設定済みのすべてのリスナーに使用できます。

ベース識別名（DN）

ディレクトリのルート レベルを「ベース」と呼びます。ベースの名前は DN（Distinguishing Name）です。Active Directory（および RFC 2247 に基づく標準）のベース DN のフォーマットでは、DNS ドメインがドメイン コンポーネント（dc=）に変換されます。たとえば、example.com のベース DN は「dc=example, dc=com」です。DNS 名の各部分が順番に表現されることに注意してください。これには、実際の LDAP 設定が反映されることも、されないこともあります。

実際に使用するディレクトリに複数のドメインが含まれている場合は、クエリの対象のベースを 1 つだけ入力するのでは不都合であることもあります。そのような場合は、LDAP サーバ設定を指定するときに、ベースを「NONE」に設定します。ただし、このように設定すると検索の効率が低下します。

LDAP クエリの構文

LDAP パス内でスペースを使用できます。引用符で囲む必要はありません。CN と DC の構文では、大文字と小文字は区別されません。

Cn=First Last,oU=user,dc=domain,DC=COM

クエリに入力する変数名では、大文字と小文字が区別されます。また、正しく動作するためには、LDAP 実装と一致している必要があります。たとえば、プロンプトで **mailLocalAddress** と入力したときに実行されるクエリは、**maillocaladdress** と入力したときとは異なります。

関連項目

- トークン: （14 ページ）

トークン:

次のトークンを LDAP クエリ内で使用できます。

- {a} ユーザ名@ドメイン名
- {d} ドメイン名

- {dn} 識別名
- {g} グループ名
- {u} ユーザ名
- {f} MAIL FROM: アドレス

（注） {f} トークンを使用できるのは、受け入れクエリーのみです。

たとえば、メールを受け入れるための Active Directory LDAP サーバに対するクエリは、次のようになります。

(|(mail={a})(proxyAddresses=smtp:{a}))

（注） 作成したクエリは、[LDAP] ページの [テスト（Test）] 機能（または **ldapconfig** コマンドの **test** サブコマンド）を使用してテストすることを強く推奨します。期待したとおりの結果が返されることを確認してから、リスナーに対して LDAP 機能をイネーブルにしてください。詳細については、LDAP クエリのテスト （19 ページ）を参照してください。

セキュア LDAP（SSL）

AsyncOS と LDAP サーバとの通信に SSL を使用するように設定できます。SSL を使用するように LDAP サーバ プロファイルを設定した場合の動作は次のようになります。

- AsyncOS は、CLI の certconfig で設定された LDAPS 証明書を使用します（自己署名証明書の作成を参照）。

  LDAP サーバによっては、LDAPS 証明書の使用をサポートするように設定する作業が必要になります。

- 設定済みの LDAPS 証明書がない場合は、デモ証明書が使用されます。

ルーティング クエリー

LDAP ルーティング クエリの再帰の制限はありません。ルーティングは完全にデータ ドリブンで行われます。ただし、AsyncOS には、ルーティングの永久ループを防止するために循環参照の有無を調べる機能があります。

LDAP サーバへの匿名のバインドをクライアントに許可する

匿名クエリを許可するように LDAP ディレクトリ サーバを設定することが必要になる場合があります。（匿名クエリを許可すると、クライアントが匿名でサーバにバインドしてクエリを実行できるようになります）。匿名クエリを許可するように Active Directory を設定する具体的な手順については、Microsoft サポート技術情報 320528 を参照してください。URL は次のとおりです。

http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B320528

または、認証とクエリ実行専用のユーザを1つ用意します。このようにすれば、任意のクライアントから匿名クエリを受け付けるように LDAP ディレクトリ サーバを開放する必要はありません。

ここでは、次の手順について説明します。

- 「匿名」認証を許可するように Microsoft Exchange 2000 サーバをセットアップする方法。
- 「匿名バインド」を許可するように Microsoft Exchange 2000 サーバをセットアップする方法。
- AsyncOS が LDAP データを Microsoft Exchange 2000 サーバから「匿名バインド」と「匿名」認証の両方を使用して取得するようにセットアップする方法。

ユーザ電子メールアドレスを問い合わせるという目的で「匿名」または「匿名バインド」認証を許可するには、Microsoft Exchange 2000 サーバに対して特定のアクセス許可を設定する必要があります。このような設定が非常に役立つのは、SMTP ゲートウェイに対する着信メールメッセージの有効性を検証するために LDAP クエリを使用する場合です。

関連項目

- 匿名認証のセットアップ （16 ページ）
- Active Directory の匿名バインドのセットアップ （17 ページ）
- Active Directory の実装に関する注意 （19 ページ）

匿名認証のセットアップ

ここで説明するセットアップ手順を実行すると、Microsoft Windows Active Directory 内の Active Directory サーバおよび Exchange 2000 サーバに対する未認証のクエリで特定のデータを使用できるようになります。Active Directory への「匿名バインド」を許可する手順については、Active Directory の匿名バインドのセットアップ （17 ページ）を参照してください。

手順

ステップ 1 必要となる Active Directory アクセス許可を確認します。

ADSI Edit スナップインまたは LDP ユーティリティを使用して、以下の Active Directory オブジェクトの属性に対するアクセス許可を修正する必要があります。

- クエリの対象であるドメインの、ドメイン名前付けコンテキストのルート。
- 電子メール情報クエリの対象であるユーザが属している OU および CN オブジェクトのすべて。

次の表に、必要なコンテナすべてに適用されている必要のあるアクセス許可を示します。

ユーザオブジェクト	権限（Permissions）	継承	アクセス許可のタイプ
全員	内容の一覧表示	コンテナオブジェクト	オブジェクト
全員	内容の一覧表示	組織単位オブジェクト	オブジェクト
全員	パブリック インフォメーション読み取り	ユーザ オブジェクト	プロパティ
全員	電話とメールのオプションの読み取り	ユーザ オブジェクト	プロパティ

ステップ 2 Active Directory のアクセス許可を設定します。

- Windows 2000 Support Tools から ADSIEdit を開きます。
- [ドメインネーミングコンテキスト（Domain Naming Context）] フォルダを見つけます。このフォルダに、ドメインの LDAP パスがあります。
- [ドメインネーミングコンテキスト（Domain Naming Context）] フォルダを右クリックして [プロパティ（Properties）] をクリックします。
- [セキュリティ（Security）] をクリックします。
- [詳細設定（Advanced）] をクリックします。
- [追加（Add）] をクリックします。
- ユーザ オブジェクト [全員（Everyone）] をクリックして [OK] をクリックします。
- [権限の種類（Permission Type）] タブをクリックします。
- [適用（Apply onto）] ボックスの [継承（Inheritance）] をクリックします。
- [権限（Permission）] アクセス許可の [許可（Allow）] チェックボックスをオンにします。

ステップ 3 Cisco メッセージング ゲートウェイの設定

コマンドライン インターフェイス（CLI）の **ldapconfig** を使用して、次の情報を指定した LDAP サーバ エントリを作成します。

- Active Directory または Exchange サーバのホスト名
- ポート 3268（Port 2）
- ドメインのルート名前付けコンテキストに一致するベース DN
- 認証タイプ：匿名

Active Directory の匿名バインドのセットアップ

ここで説明するセットアップ手順を実行すると、Microsoft Windows Active Directory 内の Active Directory サーバおよび Exchange 2000 サーバに対する匿名バインド クエリで特定のデータを使用できるようになります。Active Directory サーバの匿名バインドにより、ユーザ名 anonymous とブランクのパスフレーズが送信されます。

（注） 匿名バインドを試行するときに何らかのパスフレーズが Active Directory サーバに送信されると、認証に失敗することがあります。

手順

ステップ 1 必要となる Active Directory アクセス許可を確認します。

ADSI Edit スナップインまたは LDP ユーティリティを使用して、以下の Active Directory オブジェクトの属性に対するアクセス許可を修正する必要があります。

- クエリの対象であるドメインの、ドメイン名前付けコンテキストのルート。
- 電子メール情報クエリの対象であるユーザが属している OU および CN オブジェクトのすべて。

次の表に、必要なコンテナすべてに適用されている必要のあるアクセス許可を示します。

ユーザオブジェクト	権限（Permissions）	継承	アクセス許可のタイプ
匿名ログオン	内容の一覧表示	コンテナオブジェクト	オブジェクト
匿名ログオン	内容の一覧表示	組織単位オブジェクト	オブジェクト
匿名ログオン	パブリック インフォメーション読み取り	ユーザ オブジェクト	プロパティ
匿名ログオン	電話とメールのオプションの読み取り	ユーザ オブジェクト	プロパティ

ステップ 2 Active Directory のアクセス許可を設定します。

- Windows 2000 Support Tools から ADSIEdit を開きます。
- [ドメインネーミングコンテキスト（Domain Naming Context）] フォルダを見つけます。このフォルダに、ドメインの LDAP パスがあります。
- [ドメインネーミングコンテキスト（Domain Naming Context）] フォルダを右クリックして [プロパティ（Properties）] をクリックします。
- [セキュリティ（Security）] をクリックします。
- [詳細設定（Advanced）] をクリックします。
- [追加（Add）] をクリックします。
- ユーザ オブジェクト [匿名ログオン（ANONYMOUS LOGON）] をクリックして [OK] をクリックします。
- [権限の種類（Permission Type）] タブをクリックします。
- [適用（Apply onto）] ボックスの [継承（Inheritance）] をクリックします。
- [権限（Permission）] アクセス許可の [許可（Allow）] チェックボックスをオンにします。

ステップ 3 Cisco メッセージング ゲートウェイの設定

[システム管理（System Administration）] > [LDAP] ページ（または CLI の **ldapconfig**）を使用して、次の情報を設定した LDAP サーバ エントリを作成します。

- Active Directory または Exchange サーバのホスト名
- ポート 3268（Port 2）
- ドメインのルート名前付けコンテキストに一致するベース DN
- 認証タイプ：パスフレーズ ベース（cn=anonymous をユーザとして使用し、パスフレーズはブランク）

Active Directory の実装に関する注意

- Active Directory サーバが LDAP 接続を受け付けるポートは、3268 と 389 です。グローバル カタログへのアクセス用のデフォルト ポートは 3268 です。
- Active Directory サーバが LDAPS 接続を受け付けるポートは、636 と 3269 です。Microsoft 製品で LDAPS がサポートされるのは、Windows Server 2003 以上です。
- アプライアンスは、グローバル カタログでもあるドメイン コントローラに接続してください。これは、複数のベースに対するクエリを同じサーバを使用して実行できるようにするためです。
- クエリを正常に実行するには、Active Directory の中で、ディレクトリ オブジェクトに対する読み取り許可をグループ「Everyone」に付与する必要があります。これには、ドメイン名前付けコンテキストのルートも含まれます。
- 一般的に、多くの Active Directory 実装では、mail 属性エントリに一致する値の「ProxyAddresses」属性エントリが存在します。
- Microsoft Exchange 環境が同じインフラストラクチャ内に複数あり、互いを認識している場合は、Exchange 環境の間でメールをルーティングするときに、送信元 MTA に戻る方向のルートは通常は必要ありません。

LDAP クエリのテスト

[LDAPサーバ プロファイルを追加/編集（Add/Edit LDAP Server Profile）] ページの [クエリのテスト（Test Query）] ボタン（または CLI の `test` サブコマンド）を使用して、クエリ タイプごとに、設定した LDAP サーバに対するクエリをテストします。結果が表示されるだけでなく、クエリ接続テストの各ステージの詳細も表示されます。テストは、クエリ タイプのそれぞれに対して行うことができます。

`ldaptest` コマンドは、次の例のようにバッチ コマンドとして使用できます。

```
ldaptest LDAP.ldapaccept foo@ironport.com
```

LDAP サーバ属性の [ホスト名（Host Name）] フィールドに複数のホストを入力した場合は、各 LDAP サーバに対してクエリのテストが行われます。

表 *1: LDAP* クエリのテスト

クエリのタイプ	受信者が一致する場合（PASS）	受信者が一致しない場合（FAIL）
受信者受け入れ（[承認（Accept）]、ldapaccept）	メッセージを受け入れます。	受信者が無効：カンバセーションまたは遅延バウンスまたはメッセージをドロップ（リスナー設定による）。DHAP：ドロップ。
ルーティング（[ルーティング（Routing）]、ldaprouting）	クエリの設定に基づいてルーティングします。	このメッセージの処理を続行します。
マスカレード（[マスカレード（Masquerade）]、masquerade）	クエリ内で定義された変数マッピングに従ってヘッダーを変更します。	このメッセージの処理を続行します。
グループ メンバーシップ（[グループ（Group）]、ldapgroup）	メッセージフィルタ ルールに対して「true」を返します。	メッセージフィルタ ルールに対して「false」を返します。
SMTP Auth（[SMTP認証（SMTP Authentication）]、smtpauth）	LDAP サーバから返されたパスフレーズを使用して認証を行います。つまり、SMTP 認証が行われます。	一致するパスフレーズなし：SMTP 認証の試行は失敗します。
外部認証（externalauth）	バインド、ユーザ レコード、およびユーザのグループ メンバーシップに対して個別に「match positive」が返されます。	バインド、ユーザ レコード、およびユーザのグループ メンバーシップに対して個別に「match negative」が返されます。
スパム隔離へのエンドユーザ認証（isqauth）	エンドユーザ アカウントに対して「match positive」が返されます。	一致するパスフレーズなし：エンドユーザ認証の試行は失敗します。
スパム隔離のエイリアス統合（isqalias）	統合されたスパム通知の送信先である電子メール アドレスが返されます。	スパム通知を統合できません。

（注） クエリに入力する変数名では、大文字と小文字が区別されます。また、正しく動作するためには、LDAP 実装と一致している必要があります。たとえば、プロンプトで **mailLocalAddress** と入力したときに実行されるクエリは、**maillocaladdress** と入力したときとは異なります。シスコは、作成したすべてのクエリについて ldapconfig コマンドの test サブコマンドを使用してテストし、正しい結果が返されることを確認するよう強く推奨します。

LDAP サーバへの接続のトラブルシューティング

LDAP サーバがアプライアンスから到達不能である場合は、次のエラーのいずれかが表示されます。

- `Error: LDAP authentication failed: <LDAP Error "invalidCredentials" [0x31]>`
- `Error: Server unreachable: unable to connect`
- `Error: Server unreachable: DNS lookup failure`

サーバが到達不能になる原因としては、サーバ設定で入力されたポートの誤りや、ファイアウォールでポートが開いていないことが考えられます。LDAP サーバの通信には一般に、ポート 3268 または 389 が使用されます。Active Directory は、ポート 3268 を使用して、マルチサーバ環境で使用されるグローバル カタログにアクセスします（詳細については、付録の「ファイアウォール情報」を参照してください）。AsyncOS 4.0 では、SSL を使用して（通常はポート 636 で） LDAP サーバと通信する機能が追加されました。詳細については、セキュア LDAP（SSL） （15 ページ）を参照してください。

サーバが到達不能になる原因としてはその他に、入力されたホスト名が解決不可能であることが考えられます。

[LDAP サーバ プロファイルを追加/編集（Add/Edit LDAP Server Profile）]ページの [テスト サーバ（Test Server(s)）]（または CLI の `ldapconfig` コマンドの `test` サブコマンド）を使用して、LDAP サーバへの接続をテストできます。詳細については、LDAP サーバのテスト （7 ページ）を参照してください。

LDAP サーバが到達不能である場合：

- LDAP受け入れまたはマスカレードまたはルーティングがワーク キューに対してイネーブルになっている場合は、メールはワーク キュー内に留まります。
- LDAP 受け入れはイネーブルになっておらず、他のクエリ（グローバル ポリシー チェックなど）がフィルタ内で使用されている場合は、そのフィルタの評価結果が false になります。

受信者検証で受け入れクエリを使用する

既存のLDAPインフラストラクチャを使用して、着信メッセージ（パブリック リスナーでの）の受信者メール アドレスの扱い方を定義できます。ディレクトリ内のユーザ データに対する変更は、次回アプライアンスがディレクトリ サーバに対してクエリを実行したときに更新され

ます。キャッシュのサイズと、アプライアンスが取得したデータを保持する時間の長さは設定可能です。

（注） 特別な受信者（たとえば administrator@example.com）に対して LDAP 受け入れクエリをバイパスすることもできます。このように設定するには、受信者アクセステーブル（RAT）を使用します。この設定の方法については、「Configuring the Gateway to Receive Email」の章を参照してください。

関連項目

- 受け入れクエリの例 （22 ページ）
- Lotus Notes の場合の受け入れクエリの設定 （23 ページ）

受け入れクエリの例

次の表に、受け入れクエリの例を示します。

表 *2:* 一般的な *LDAP* 実装での *LDAP* クエリ文字列の例：受け入れ

クエリの対象	受信者検証

OpenLDAP	`(mailLocalAddress={a})`
	`(mail={a})`
	`(mailAlternateAddress={a})`

Microsoft Active Directory Address Book **Microsoft Exchange**	`(|(mail={a})(proxyAddresses=smtp:{a}))`

Sun ONE Directory Server	`(mail={a})`
	`(mailAlternateAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailForwardingAddress={a})`
	`(mailRoutingAddress={a})`

Lotus Notes/Lotus Domino	`(|(|(mail={a})(uid={u}))(cn={u}))` `(|(ShortName={u})(InternetAddress={a})(FullName={u}))`

ユーザ名（左側）の検証を行うこともできます。このことが役に立つのは、ディレクトリに格納されていないドメインのメールも受け入れるようにしたい場合です。受け入れクエリを (uid={u}) に設定してください。

Lotus Notes の場合の受け入れクエリの設定

LDAPACCEPT と Lotus Notes とを組み合わせる場合は、注意が必要です。Notes LDAP に格納されているユーザの属性が次のように設定されているとします。

```
mail=juser@example.com

cn=Joe User

uid=juser

cn=123456

location=New Jersey
```

LDAP ディレクトリに存在しないユーザであるにもかかわらず、Lotus はこのユーザへの電子メールを、指定されたアドレス以外の形式（たとえばJoe_User@example.com）であっても受け入れます。したがって、AsyncOS は、このユーザの有効なユーザ メール アドレスをすべて見つけることはできません。

この解決策の 1 つは、他の形式のアドレスのパブリッシュを試みるというものです。詳細については、Lotus Notes 管理者に問い合わせてください。

複数ターゲットアドレスへのメール送信にルーティング クエリを使用する

AsyncOS では、エイリアス拡張（複数ターゲット アドレスへの LDAP ルーティング）がサポートされます。AsyncOS によって、元のメール メッセージはエイリアス ターゲットごとに別の新しいメッセージで置き換えられます（たとえば、recipient@yoursite.com へのメッセージは、newrecipient1@hotmail.com や recipient2@internal.yourcompany.com などへの、それぞれ独立したメッセージで置き換えられます）。ルーティング クエリは、他の電子メール処理システムではエイリアシング クエリと呼ばれることもあります。

関連項目

- ルーティング クエリの例 （23 ページ）

ルーティング クエリの例

表 *3:* 一般的な *LDAP* 実装での *LDAP* クエリー文字列の例：ルーティング

クエリの対象	別のメールホストへのルーティング
OpenLDAP	`(mailLocalAddress={a})`

クエリの対象	別のメールホストへのルーティング
Microsoft Active Directory Address Book **Microsoft Exchange**	該当しない可能性あり

Sun ONE Directory Server	`(mail={a})`
	`(mailForwardingAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailRoutingAddress={a})`
	`(otherMailbox={a})`
	`(rfc822Mailbox={a})`

Active Directory の実装によっては、`proxyAddresses` 属性のエントリが複数存在することがありますが、この属性の値は Active Directory によって `smtp:user@domain.com` という形式で格納されるため、このデータは LDAP ルーティング/エイリアス拡張には使用できません。ターゲットアドレスはそれぞれ別の `attribute:value` ペアに存在する必要があります。Microsoft Exchange 環境が同じインフラストラクチャ内に複数あり、互いを認識している場合は、Exchange 環境の間でメールをルーティングするときに、送信元 MTA に戻る方向のルートは通常は必要ありません。

関連項目

- ルーティング：MAILHOST と MAILROUTINGADDRESS （24 ページ）

ルーティング：MAILHOST と MAILROUTINGADDRESS

ルーティング クエリの場合は、MAILHOST の値は IP アドレスではなく、解決可能なホスト名であることが必要です。これには、内部的な DNSconfig が必要になるのが一般的です。

MAILHOST は、ルーティング クエリでは省略可能です。MAILROUTINGADDRESS は、MAILHOST が設定されていない場合は必須です。

エンベロープ送信者を書き換えるためのマスカレードクエリの使用

マスカレードとは、電子メールのエンベロープ送信者（「送信者」または「MAIL FROM」と呼ばれることもあります）および To:、From:、CC: の各ヘッダーを、定義済みのクエリに基づいて書き換える機能です。この機能の一般的な実装例の 1 つが「仮想ドメイン」であり、これによって複数のドメインを 1 つのサイトからホスティングできるようになります。他の一般的な実装としては、ネットワーク インフラストラクチャを「隠す」ために、電子メールヘッダーの文字列からサブドメインを取り除く（「ストリッピング」）というものがあります。

関連項目

- マスカレード クエリの例 （25 ページ）
- 「フレンドリ名」のマスカレード （25 ページ）

マスカレード クエリの例

表 *4 :* 一般的な *LDAP* 実装での *LDAP* クエリー文字列の例：マスカレード

クエリの対象	マスカレード
OpenLDAP	`(mailRoutingAddress={a})`
Microsoft Active Directory Address Book	`(proxyaddresses=smtp:{a})`

Sun ONE Directory Server	`(mail={a})`
	`(mailAlternateAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailForwardingAddress={a})`
	`(mailRoutingAddress={a})`

「フレンドリ名」のマスカレード

ユーザ環境によっては、LDAP ディレクトリ サーバ スキーマの中に、メール ルーティング アドレスやローカル メール アドレス以外に「フレンドリ名」が含まれていることがあります。AsyncOS では、エンベロープ送信者（発信メールの場合）やメッセージ ヘッダー（受信メールの場合、To:、Reply To:、From:、CC: など）を、この「フレンドリ名」でマスカレードできます。フレンドリ アドレスには、有効な電子メール アドレスでは通常は許可されない特殊文字（引用符、スペース、カンマなど）が含まれていてもかまいません。

LDAP クエリ経由でヘッダーをマスカレードするときに、フレンドリ メール文字列全体を LDAP サーバからの結果で置き換えるかどうかを設定時に選択できます。この動作がイネーブルになっていても、エンベロープ送信者には user@domain 部分のみが使用されることに注意してください（フレンドリ名はルールに反するため）。

標準的な LDAP マスカレードのときと同様に、LDAP クエリの結果が空（長さが 0 またはすべてホワイト スペース）の場合は、マスカレードは行われません。

この機能をイネーブルにするには、LDAP ベースのマスカレード クエリをリスナーに対して設定するときに（[LDAP] ページまたは `ldapconfig` コマンド）、次の質問に対して「y」と回答します。

```
Do you want the results of the returned attribute to replace the entire
friendly portion of the original recipient? [N]
```

たとえば、次のような LDAP エントリがあるとします。

属性	値
mailRoutingAddress	admin\@example.com
mailLocalAddress	joe.smith\@example.com
mailFriendlyAddress	“Administrator for example.com,” <joe.smith\@example.com>

この機能がイネーブルになっている場合に、LDAP クエリが (mailRoutingAddress={a}) で、マスカレード属性が (mailLocalAddress) ならば、次のように置き換えられます。

元のアドレス（From、To、CC、Reply-to）	マスカレードされたヘッダー	マスカレードされたエンベロープ送信者
admin@example.com	From: “Administrator for example.com,” <joe.smith@example.com>	MAIL FROM: <joe.smith@example.com>

受信者がグループメンバーであるかどうかを判別するグループ LDAP クエリの使用

LDAP ディレクトリ内で定義されたグループに受信者が属しているかどうかを、LDAP サーバに対するクエリを使用して判別できます。

手順

ステップ 1 メッセージに rcpt-to-group または mail-from-group ルールを適用するメッセージ フィルタを作成します。

ステップ 2 次に、[システム管理（System Administration）] > [LDAP] ページ（または **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、グループ メンバーシップを調べるクエリーを設定します。

ステップ 3 [ネットワーク（Network）] > [リスナー（Listeners）] ページ（または **listenerconfig -> edit -> ldapgroup** サブコマンド）を使用して、このグループ クエリーをリスナーに対して有効にします。

次のタスク

関連項目

- グループ クエリの例 （27 ページ）
- グループ クエリの設定 （27 ページ）

グループ クエリの例

表 *5:* 一般的な *LDAP* 実装での *LDAP* クエリ文字列の例：グループ

クエリの対象	グループ
OpenLDAP	OpenLDAP では、memberOf 属性はデフォルトではサポートされません。LDAP 管理者によって、この属性または類似の属性がスキーマに追加されていることがあります。
Microsoft Active Directory	`(&(memberOf={g})(proxyAddresses=smtp:{a}))`
Sun ONE Directory Server	`(&(memberOf={g})(mailLocalAddress={a}))`

たとえば、LDAP ディレクトリで「マーケティング」グループのメンバーが ou=Marketing と分類されているとします。この分類を使用して、このグループが送受信するメールを特別な方法で取り扱うことができます。ステップ 1 で、メッセージに作用するメッセージ フィルタを作成し、ステップ 2 と 3 で LDAP ルックアップ メカニズムをイネーブルにします。

グループ クエリの設定

次に示す例では、マーケティング グループ（LDAP グループ「Marketing」として定義）のメンバーからのメールを代替メール配信ホスト `marketingfolks.example.com` に配信します。

手順

ステップ 1 初めに、グループ メンバーシップに関して肯定的に一致するメッセージに作用する、メッセージ フィルタを作成します。この例では、作成するフィルタの中で `mail-from-group` ルールを使用します。メッセージのうち、エンベロープ送信者が LDAP グループ「marketing-group1」に属していることが判明したものはすべて、代替配信ホストに送信されます（フィルタの `alt-mailhost` アクション）。

グループ メンバーシップ フィールド変数（groupName）は、ステップ 2 で定義します。グループ属性「groupName」の値は、`marketing-group1` と定義されます。

```
mail3.example.com> filters


Choose the operation you want to perform:

- NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new

Enter filter script. Enter '.' on its own line to end.

MarketingGroupfilter:
```

```
if (mail-from-group == "marketing-group1") {

alt-mailhost ('marketingfolks.example.com');}

.

1 filters added.

Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]>
```

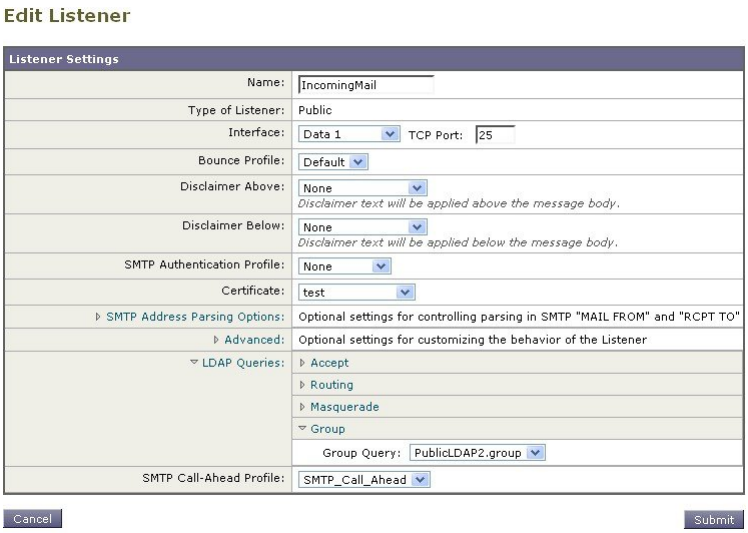
メッセージ フィルタ ルール `mail-from-group` と `rcpt-to-group` の詳細については、メッセージ フィルタ ルールを参照してください。

ステップ 2 次に、[LDAPサーバプロファイルを追加（Add LDAP Server Profile）] ページを使用して、アプライアンスのバインド先となる LDAP サーバを定義し、グループ メンバーシップを調べる最初のクエリを定義します。

ステップ 3 次に、パブリック リスナー「InboundMail」で LDAP クエリを使用してグループ ルーティングを行うように更新します。[リスナーを編集（Edit Listener）] ページを使用して、前のステップで指定した LDAP クエリをイネーブルにします。

このクエリが実行されると、リスナーが受け入れたメッセージによって LDAP サーバに対するクエリがトリガーされて、グループ メンバーシップが特定されます。PublicLDAP2.group クエリはすでに、[システム管理（System Administration）] > [LDAP] ページで定義されています。

図 *6:* リスナーでのグループ クエリの指定



ステップ 4 変更を送信し、保存します。

例：グループクエリを使用してスパムとウイルスのチェックをスキップする

メッセージ フィルタはパイプラインの初めの方で実行されるので、グループ クエリを使用すると、特定のグループについてウイルスとスパムのチェックをスキップできます。たとえば、社内の IT グループへのメッセージについては、スパムとウイルスのチェックをスキップしてすべて受信したいという要望があるとします。LDAP レコードの中に、DN をグループ名として使用するグループエントリを作成します。このグループ名は、次の DN エントリで構成されます。

cn=IT, ou=groups, o=sample.com

LDAP サーバ プロファイルを作成し、次のグループ クエリを指定します。

(&(memberOf={g})(proxyAddresses=smtp:{a}))

次に、このクエリをリスナーに対してイネーブルにします。これで、メッセージがそのリスナーで受信されたときに、このグループ クエリがトリガーされます。

IT グループのメンバーについてはウイルスとスパムのチェックをスキップするために、次のメッセージ フィルタを作成して、着信メッセージを LDAP グループと比較して検査します。

```
[]> - NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new

Enter filter script. Enter '.' on its own line to end.
```

```
IT_Group_Filter:

if (rcpt-to-group == "cn=IT, ou=groups, o=sample.com"){

skip-spamcheck();

skip-viruscheck();

deliver();

}

.
1 filters added.
```

（注） このメッセージ フィルタ内の rcpt-to-group には、グループ名として入力された DN（cn=IT, ou=groups, o=sample.com）が反映されています。メッセージ フィルタ内で使用しているグループ名が正しいことを確認してください。フィルタの実行時に、LDAP ディレクトリ内でその名前との比較が確実に行われるようにするためです。

リスナーが受け入れたメッセージによってLDAPサーバに対するクエリがトリガーされて、グループ メンバーシップが特定されます。メッセージ受信者がITグループのメンバーの場合は、メッセージフィルタの定義に従ってウイルスとスパムのチェックがいずれもスキップされて、メッセージが受信者に配信されます。フィルタで LDAP クエリの結果をチェックするには、LDAP サーバに対する LDAP クエリを作成し、その LDAP クエリをリスナーに対してイネーブルにする必要があります。

特定のドメインヘルーティングするためのドメインベース クエリの使用

ドメインベース クエリとは、LDAP クエリをタイプ別にグループ化し、特定のドメインに関連付けたうえで、特定のリスナーに割り当てたものです。ドメインベース クエリが使用されるのは、複数の LDAP サーバがそれぞれ異なるドメインに関連付けられているが、すべての LDAP サーバに対するクエリを同じリスナー上で実行する場合です。たとえば、「MyCompany」という会社が「HisCompany」と「HerCompany」の 2 社を買収するとします。MyCompany は自社のドメイン MyCompany.example.com に加えて HisCompany.example.com および HerCompany.example.com のドメインを運用すると共に、ドメインごとに別の LDAP サーバを運用して、各ドメインに関連付けられた従業員の情報を格納しています。この 3 つのドメインのメールをすべて受け入れるために、MyCompany はドメインベース クエリを作成します。これで、MyCompany.example.com は Mycompany.example.com、HisCompany.example.com、および HerCompany.example.com のメールを同じリスナー上で受け入れることができます。

手順

ステップ 1 ドメインベース クエリで使用するドメインごとに 1 つずつ、サーバ プロファイルを作成します。このサーバ プロファイルのそれぞれに対して、ドメインベース クエリに使用するクエリを設定します（受け入れ、ルーティングなど）。詳細については、LDAP サーバに関する情報を格納する LDAP サーバ プロファイルの作成 （5 ページ）を参照してください。

ステップ 2 ドメインベース クエリを作成します。ドメインベース クエリを作成するときは、各サーバ プロファイルからクエリを選択します。また、どのクエリを実行するかを Envelope To フィールドに基づいて決定するように、アプライアンスを設定します。クエリーの作成方法の詳細については、ドメインベース クエリの作成 （31 ページ） を参照してください。

ステップ 3 ドメインベース クエリをパブリックまたはプライベートのリスナーに対してイネーブルにします。リスナーの設定方法の詳細については、「Configuring the Gateway to Receive Mail」の章を参照してください。

（注） ドメインベース クエリは他にも、スパム隔離機能の LDAP エンドユーザ アクセスやスパム通知のために使用できます。詳細については、「スパム隔離」の章を参照してください。

次のタスク

関連項目

- ドメインベース クエリの作成 （31 ページ）

ドメインベース クエリの作成

ドメインベース クエリは、[システム管理（System Administration）] > [LDAP] > [LDAPサーバ プロファイル（LDAP Server Profiles）] ページで作成します。

手順

ステップ 1 [LDAPサーバプロファイル（LDAP Server Profiles）] ページの [詳細設定（Advanced）] をクリックします。

ステップ 2 [ドメイン割り当ての追加（Add Domain Assignments）] をクリックします。

ステップ 3 ドメインベース クエリーの名前を入力します。

ステップ 4 クエリー タイプを選択します。

（注） ドメインベース クエリを作成するときに選択するクエリのタイプは、すべて同じでなければなりません。クエリ タイプを選択すると、アプライアンスはそのタイプのクエリを利用可能なサーバ プロファイルから取得し、クエリ フィールドを生成します。

ステップ 5 [ドメイン割り当て（Domain Assignments）] フィールドに、ドメインを入力します。

ステップ 6 このドメインに関連付けるクエリーを選択します。

ステップ 7 クエリのドメインがすべて追加されるまで、行を追加します。

ステップ 8 どのクエリにも一致しないときに実行する、デフォルトのクエリを入力できます。デフォルトクエリーを入力しない場合は、[なし（None）] を選択します。

ステップ 9 クエリをテストします。[クエリのテスト（Test Query）] ボタンをクリックし、テストするユーザ ログインとパスフレーズまたはメール アドレスを [テスト パラメータ（Test Parameters）] のフィールドに入力します。結果が [接続ステータス（Connection Status）] フィールドに表示されます。

ステップ 10 （省略可能）{f} トークンを受け入れクエリ内で使用する場合は、エンベロープ送信者アドレスをテスト クエリに追加できます。

（注） ドメインベース クエリの作成が終了したら、このクエリをパブリックまたはプライベートのリスナーに関連付ける必要があります。

ステップ 11 変更を送信し、保存します。

一連の LDAP クエリを実行するためのチェーン クエリの使用

チェーン クエリは、アプライアンスによって順番に実行が試行される一連の LDAP クエリで構成されます。アプライアンスは、この「チェーン」の中の各クエリの実行を試行し、LDAP サーバから肯定的なレスポンスが返されると（または「チェーン」の最後のクエリで否定的なレスポンスが返されるか失敗すると）実行を停止します。チェーン ルーティング クエリーでは、アプライアンスは書き換えられた電子メールアドレスごとに、同じ設定の一連のチェーンクエリーを再実行します。チェーン クエリが役立つのは、LDAP ディレクトリ内のエントリにおいて、さまざまな属性に類似の（または同一の）値が格納されている場合です。たとえば、属性 maillocaladdress と mail がユーザ電子メール アドレスを格納するために使用されているとします。この両方の属性に対して確実にクエリを実行するには、チェーン クエリを使用します。

手順

ステップ 1 チェーン クエリ内で使用するクエリごとに、サーバ プロファイルを作成します。このサーバ プロファイルのそれぞれについて、チェーン クエリーに使用するクエリーを設定します。詳細については、LDAP サーバに関する情報を格納する LDAP サーバ プロファイルの作成 （5 ページ）を参照してください。

ステップ 2 チェーン クエリを作成します。詳細については、チェーン クエリの作成 （33 ページ）を参照してください。

ステップ 3 チェーン クエリをパブリックまたはプライベートのリスナーに対してイネーブルにします。リスナーの設定方法の詳細については、「Configuring the Gateway to Receive Mail」の章を参照してください。

（注） ドメインベース クエリは他にも、スパム隔離機能の LDAP エンドユーザ アクセスやスパム通知のために使用できます。詳細については、「スパム隔離」の章を参照してください。

次のタスク

関連項目

- チェーン クエリの作成 （33 ページ）

チェーン クエリの作成

チェーン クエリーは、[システム管理（System Administration）] > [LDAP] > [LDAPサーバプロファイル（LDAP Server Profiles）] ページで作成します。

手順

ステップ 1 [LDAPサーバプロファイル（LDAP Server Profiles）] ページの [詳細設定（Advanced）] をクリックします。

ステップ 2 [チェーン クエリを追加（Add Chain Query）] をクリックします。

ステップ 3 チェーン クエリの名前を入力します。

ステップ 4 クエリー タイプを選択します。

チェーンクエリを作成するときに選択するクエリのタイプは、すべて同じでなければなりません。クエリ タイプを選択すると、アプライアンスはそのタイプのクエリを利用可能なサーバプロファイルから取得し、クエリ フィールドを生成します。

ステップ 5 チェーン クエリに追加するクエリを選択します。

アプライアンスによって、ここで設定した順にクエリが実行されます。したがって、複数のクエリをチェーンクエリに追加する場合は、より限定的なクエリの後でより汎用のクエリが実行されるような順序にすることを推奨します。

ステップ 6 クエリをテストします。[クエリのテスト（Test Query）] ボタンをクリックし、テストするユーザ ログインとパスフレーズまたはメール アドレスを [テスト パラメータ（Test Parameters）] のフィールドに入力します。結果が [接続ステータス（Connection Status）] フィールドに表示されます。

ステップ 7 （省略可能）{f} トークンを受け入れクエリ内で使用する場合は、エンベロープ送信者アドレスをテスト クエリに追加できます。

（注） チェーンクエリの作成が終了したら、このクエリをパブリックまたはプライベートのリスナーに関連付ける必要があります。

ステップ 8 変更を送信し、保存します。

LDAP によるディレクトリ ハーベスト攻撃防止

ディレクトリ ハーベスト攻撃は、悪意のある送信者が、よくある名前を持つ受信者宛にメッセージを送信することによって開始します。電子メール ゲートウェイは、受信者がその場所に有効なメールボックスを持っているかどうかを調べて応答を返します。これを大量に実行すると、悪意のある送信者は、どのアドレスにスパムを送信すればよいかを、有効なアドレスの「収穫（ハーベスト）」によって特定できるようになります。

E メールセキュリティ アプライアンスでは、LDAP 受け入れ検証クエリーを使用すると、ディレクトリ ハーベスト攻撃（DHA）を検出して防止できます。LDAP 受け入れを設定するときに、ディレクトリ ハーベスト攻撃防止を SMTP カンバセーション中に行うか、ワーク キューの中で行うかを選択できます。

関連項目

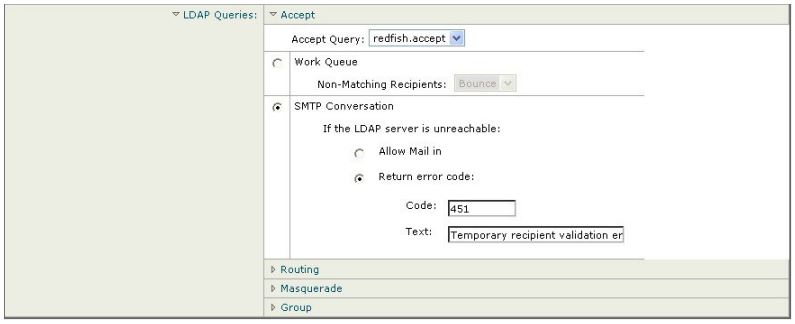
- SMTP カンバセーション中のディレクトリ ハーベスト攻撃防止 （34 ページ）
- 作業キュー内でのディレクトリ ハーベスト攻撃防止 （36 ページ）

SMTP カンバセーション中のディレクトリ ハーベスト攻撃防止

DHA を防止するには、ドメインだけを Recipient Access Table（RAT; 受信者アクセス テーブル）に入力しておき、LDAP 受け入れ検証を SMTP カンバセーション内で実行します。

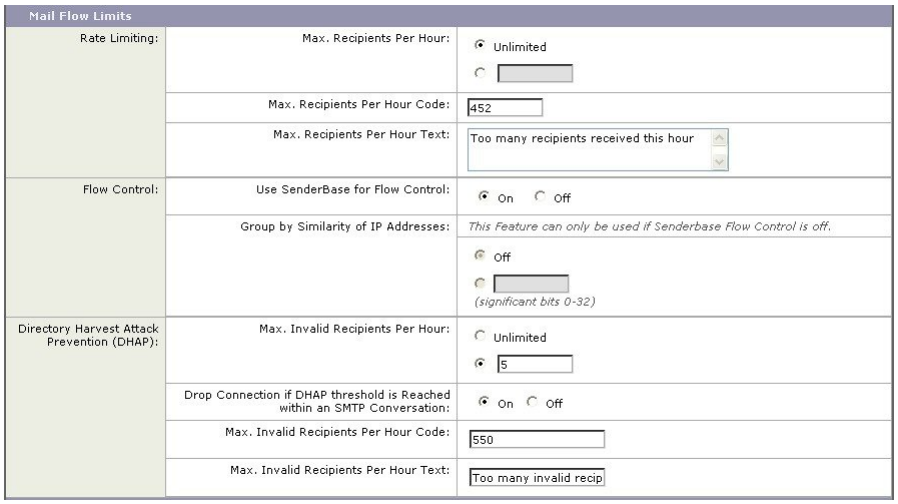
SMTP カンバセーション中にメッセージをドロップするには、LDAP 受け入れのための LDAP サーバ プロファイルを設定します。次に、LDAP 受け入れクエリを SMTP カンバセーション中に実行するようにリスナーを設定します。

図 *7:* 受け入れクエリを *SMTP* カンバセーション中に実行するように設定



リスナーで実行する LDAP 受け入れクエリを設定したら、そのリスナーに関連付けられたメール フロー ポリシーの中の DHAP（ディレクトリ ハーベスト攻撃防止）設定を指定する必要があります。

図 *8 : SMTP* カンバセーション中に接続をドロップするようにメール フロー ポリシーを設定する



リスナーに関連付けられたメール フロー ポリシーの中で、ディレクトリ ハーベスト攻撃防止のための次の項目を設定します。

- [1時間あたりの無効な受信者の最大数（Max. Invalid Recipients Per hour）]。このリスナーがリモート ホストから受け取る無効な受信者の 1 時間あたりの最大数です。このしきい値は、RAT 拒否の総数を表します。これは、無効な LDAP 受信者宛てのため SMTP カンバセーション中にドロップされたメッセージの総数と、ワーク キュー内でバウンスされたメッセージの合計です。たとえば、しきい値を 5 と設定した場合に、検出された RAT 拒否が 2 件で、無効な LDAP 受信者宛てのためドロップされたメッセージが 3 件であるとします。この時点で、アプライアンスはしきい値に到達したと判断して、接続をドロップさせます。デフォルトでは、パブリック リスナーでの 1 時間あたりの受信者の最大数は 25 です。プライベート リスナーの場合は、1 時間あたりの受信者の最大数はデフォルトでは無制限です。この最大数を [無制限（Unlimited）] に設定すると、そのメール フロー ポリシーに対して DHAP はイネーブルになりません。
- [SMTP 対話内で DHAP しきい値に到達した場合、接続をドロップ（Drop Connection if DHAP Threshold is reached within an SMTP conversation）]。ディレクトリ ハーベスト攻撃防止のしきい値に達したときにアプライアンスによって接続をドロップさせように設定します。
- [時間コードあたりの最大受信者数（Max. Recipients Per Hour Code）]. 接続をドロップするときに使用するコードを指定します。デフォルトのコードは 550 です。
- [時間テキストあたりの最大受信者数（Max. Recipients Per Hour Text）]。ドロップした接続に対して使用するテキストを指定します。デフォルトのテキストは「Too many invalid recipients」です。

しきい値に達した場合は、受信者が無効であってもメッセージのエンベロープ送信者にバウンス メッセージが送信されることはありません。

作業キュー内でのディレクトリ ハーベスト攻撃防止

ディレクトリ ハーベスト攻撃（DHA）のほとんどは、ドメインだけを受信者アクセス テーブル（RAT）に入力しておき、LDAP受け入れ検証をワーク キュー内で実行することによって防止できます。この方法を使用すると、悪意のある送信者が、受信者が有効かどうかをSMTPカンバセーション中に知ることはできなくなります。（受け入れクエリが設定されているときは、システムはメッセージを受け入れて、LDAP 受け入れ検証をワーク キュー内で実行します）。ただし、メッセージのエンベロープ送信者には、受信者が無効である場合にバウンスメッセージが送信されます。

関連項目

- ワーク キュー内でディレクトリ ハーベスト攻撃防止するための設定 （36 ページ）

ワーク キュー内でディレクトリ ハーベスト攻撃防止するための設定

ディレクトリ ハーベスト攻撃を防止するには、初めに LDAP サーバ プロファイルを設定して LDAP 受け入れをイネーブルにします。LDAP 受け入れクエリをイネーブルにしたら、次のように、その受け入れクエリを使用するようにリスナーを設定すると共に、受信者が一致しない場合はメールをバウンスするように指定します。

次に、メール フロー ポリシーを設定します。このポリシーでは、所定の時間内に送信 IP アドレスあたりどれだけの無効な受信者アドレスをシステムが受け入れるかを定義します。この数を超えると、システムはこの状態が DHA（ディレクトリ ハーベスト攻撃）であると判断してアラート メッセージを送信します。このアラート メッセージに含まれる情報は次のとおりです。

```
LDAP: Potential Directory Harvest Attack from host=('IP-address', 'domain_name
'), dhap_limit=n, sender_group=sender_group,


listener=listener_name, reverse_dns=(reverse_IP_address, 'domain_name
', 1), sender=envelope_sender, rcpt=envelope_recipients
```

メール フロー ポリシーで指定されたしきい値に達するまでは、システムによってメッセージがバウンスされますが、それ以降は応答を返すことなく受け入れられてドロップされます。したがって、正当な送信者にはアドレスの誤りが通知されますが、悪意のある送信者は、どの受信者が受け入れられたかを判断できません。

この無効受信者カウンタの働きは、現在 AsyncOS に実装されているレート制限機能に似ています。つまり、管理者がこの機能をイネーブルにして、上限値をパブリック リスナーの HAT 内のメール フロー ポリシーの中で設定します（HAT のデフォルトのメール フロー ポリシーを含む）。

また、コマンドライン インターフェイスで `listenerconfig` コマンドを使用して、これを設定することもできます。

この機能は、メール フロー ポリシーを GUI で編集するときにも表示されます（対応するリスナーに対して LDAP クエリが作成済みの場合）。

1 時間あたりの無効受信者数を入力すると、そのメール フロー ポリシーに対して DHAP（ディレクトリ ハーベスト攻撃防止）がイネーブルになります。デフォルトで、パブリック リスナーでは 1 時間あたり最大 25 件の無効受信者が受け入れられます。プライベート リスナーの場合は、1 時間あたりの無効受信者数はデフォルトでは無制限です。この最大数を [無制限（Unlimited）] に設定すると、そのメール フロー ポリシーに対して DHAP はイネーブルになりません。

SMTP 認証を行うための AsyncOS の設定

AsyncOS では、SMTP 認証がサポートされています。SMTP Auth は、SMTP サーバに接続するクライアントを認証するメカニズムです。

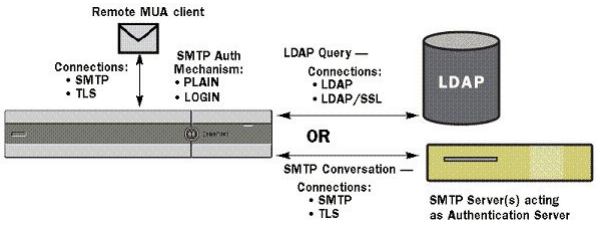
このメカニズムを利用すると、特定の組織に所属するユーザが、その組織のメール サーバにリモートで接続している（自宅や出張先などから）ときもメール サーバを使用してメールを送信できるようになります。メール ユーザ エージェント（MUA）は、メールの送信を試行するときに認証要求（チャレンジ/レスポンス）を発行できます。

SMTP 認証は、発信メール リレーに対しても使用できます。これを利用すると、アプライアンスがネットワークのエッジではない場合に、アプライアンスからリレー サーバへのセキュア接続を確立できます。

AsyncOS では、ユーザ クレデンシャルの認証方式として次の 2 つがサポートされています。

- LDAP ディレクトリを使用する。
- 別の SMTP サーバを使用する（SMTP Auth 転送と SMTP Auth 発信）。

図 *9 : SMTP Auth* のサポート：*LDAP* ディレクトリ ストアまたは *SMTP* サーバ



SMTP 認証方式を設定したら、HAT メール フロー ポリシー内で使用される SMTP Auth プロファイルを、smtpauthconfig コマンドを使用して作成します（リスナーでの SMTP 認証の有効化 （41 ページ）を参照）。

関連項目

- SMTP 認証の設定 （38 ページ）
- SMTP 認証クエリの設定 （39 ページ）
- 第 2 の SMTP サーバ経由での SMTP 認証（転送を使用する SMTP Auth） （40 ページ）
- LDAP を使用する SMTP 認証 （41 ページ）
- クライアント証明書を使用した SMTP セッションの認証 （44 ページ）
- 発信 SMTP 認証 （45 ページ）

- ロギングと SMTP 認証 （45 ページ）

SMTP 認証の設定

LDAP サーバを使用して認証を行う場合は、[LDAPサーバプロファイルを追加（Add LDAP Server Profile）] または [LDAPサーバプロファイルを編集（Edit LDAP Server Profile）] ページ（または **ldapconfig** コマンド）でクエリ タイプとして SMTPAUTH を選択して SMTP 認証クエリを作成します。設定する LDAP サーバのそれぞれについて、SMTP 認証プロファイルとして使用する SMTPAUTH クエリを 1 つ設定できます。

SMTP 認証クエリには、「LDAP バインド」と「属性としてのパスフレーズ」の 2 種類があります。「属性としてのパスフレーズ」を使用するときは、アプライアンスによってLDAPディレクトリ内のパスフレーズ フィールドが取り出されます。パスフレーズは、プレーン テキスト、暗号化、またはハッシュされて格納されている可能性があります。LDAP バインドを使用すると、アプライアンスは、クライアントによって提供された資格情報を使用してLDAP サーバにログインしようとします。

関連項目

- 属性としてのパスフレーズの指定 （38 ページ）

属性としてのパスフレーズの指定

OpenLDAP の規定（RFC 2307 に基づく）では、コーディングのタイプを中カッコで囲み、その後にエンコードされたパスフレーズを続けることになっています（たとえば「{SHA}5en6G6MezRroT3XKqkdPOmY/BfQ=」）。この例では、パスフレーズ部分はプレーンテキストのパスフレーズに SHA を適用してから base64 エンコーディングしたものです。

アプライアンスがパスフレーズを取得する前に、SASL メカニズムのネゴシエートが MUA との間で行われ、アプライアンスと MUA はどの方法を使用するかを決定します（サポートされているメカニズムはLOGIN、PLAIN、MD5、SHA、SSHA、CRYPT SASL です）。その後で、アプライアンスはLDAPデータベースに対するクエリを実行してパスフレーズを取得します。LDAP内では、中カッコで囲まれたプレフィックスがパスフレーズに付いていることがあります。

- プレフィックスが付いていない場合は、LDAP内に格納されているパスフレーズがプレーン テキストであると見なされます。
- プレフィックスが付いている場合は、アプライアンスはそのハッシュ化パスフレーズを取得し、MUA によって指定されたユーザ名とパスフレーズの両方あるいはどちらかのハッシュを実行して、ハッシュ後のパスフレーズと比較します。アプライアンスでサポートされるハッシュ タイプはSHA1 と MD5 であり、RFC 2307 の規定に基づいて、パスフレーズ フィールド内ではハッシュ化パスフレーズの前にハッシュ メカニズムのタイプが付加されます。
- LDAP サーバの中には、OpenWave LDAP サーバのように、暗号化されたパスフレーズの前に暗号化タイプを付加しないものもあり、代わりに暗号化タイプが別のLDAP属性として格納されています。このような場合は、管理者が指定したデフォルトのSMTP AUTH暗

号化方式であると見なされて、そのパスフレーズとSMTPカンバセーションで取得されたパスフレーズとが比較されます。

アプライアンスは、SMTP Auth交換から任意ユーザ名を受け取ってLDAPクエリに変換し、このクエリを使用してクリア テキストまたはハッシュ化されたパスフレーズ フィールドを取得します。次に、SMTP Authクレデンシャルで指定されたパスフレーズに対してハッシュが必要な場合は実行し、その結果をLDAPからのパスフレーズと比較します（ハッシュ タイプのタグがある場合は取り除く）。一致した場合は、SMTP Authカンバセーションが続行されます。一致しない場合は、エラー コードが返されます。

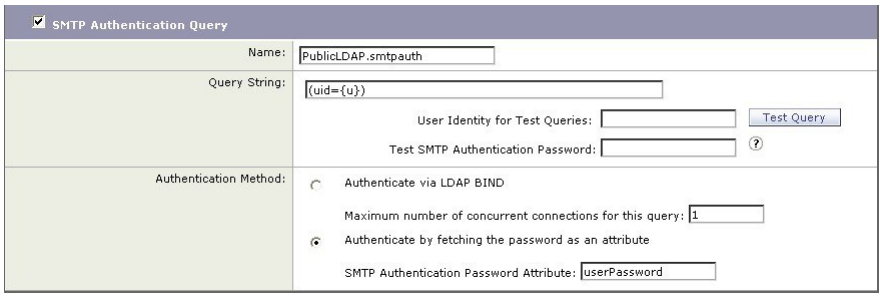
SMTP 認証クエリの設定

表 *6 : SMTP Auth LDAP* クエリのフィールド

[名前（Name）]	**クエリの名前**
クエリー文字列（Query String）	認証をLDAPバインド経由で行うか、パスフレーズを属性として取得して行うかを選択できます。 [バインド（Bind）]：LDAPサーバへのログイン試行には、クライアントによって指定されたクレデンシャルを使用します（これを「LDAPバインド」と呼びます）。 SMTP Authクエリで使用される同時接続の最大数を指定します。この数は、上のLDAPサーバ属性で指定した数を超えてはなりません。バインド認証時に大量のセッション タイムアウトが発生するのを防ぐには、ここで指定する同時接続の最大数を大きくします（一般的には、接続のほぼすべてをSMTP Authに割り当てることができます）。バインド認証ごとに、新しい接続が1つ使用されます。残りの接続は、他のタイプのLDAPクエリで共有されます。 [属性としてのパスフレーズ（Passphrase as Attribute）]：パスフレーズを取得して認証を行うには、下の[SMTP認証のパスフレーズの属性（SMTP Auth Passphrase Attribute）]フィールドでパスフレーズを指定します。 いずれかの種類の認証に使用するLDAPクエリを指定します。アクティブ ディレクトリのクエリの例：(&(samaccountname={u})(objectCategory=person)(objectClass=user))
SMTP認証のパスフレーズの属性（SMTP Auth Passphrase Attribute）	[属性としてパスフレーズを取得した認証（Authenticate by fetching the passphrase as an attribute）]を選択した場合は、パスフレーズ属性をここで指定します。

次の例では、[システム管理（System Administration）] > [LDAP]ページを使用してLDAP設定「PublicLDAP」を編集し、SMTPAUTHクエリを追加しています。クエリ文字列（uid={u}）は、userPassword属性と比較するように作成されています。

図 *10 : SMTP* 認証クエリ



SMTPAUTH プロファイルの設定が完了すると、そのクエリを SMTP 認証に使用するようにリスナーを設定できます。

第 2 の SMTP サーバ経由での SMTP 認証（転送を使用する SMTP Auth）

SMTP 認証カンバセーションのために指定されたユーザ名とパスフレーズを、別の SMTP サーバを使用して検証するようにアプライアンスを設定できます。

認証を行うサーバは、メールを転送するサーバとは別のものであり、SMTP 認証要求への応答だけを行います。認証に成功したときは、専用メール サーバによるメールの SMTP 転送を続行できます。この機能は、「転送を使用する SMTP Auth」と呼ばれることもあります。クレデンシャルのみが別の SMTP サーバに転送（プロキシ）されて認証が行われるからです。

手順

ステップ 1 [ネットワーク（Network）] > [SMTP認証（SMTP Authentication）] を選択します。

ステップ 2 [プロファイルを追加...（Add Profile...）] をクリックします。

ステップ 3 SMTP 認証プロファイルの一意の名前を入力します。

ステップ 4 [プロファイルタイプ（Profile Type）] で [転送（Forward）] を選択します。

ステップ 5 [Next] をクリックします。

ステップ 6 転送サーバのホスト名/IP アドレスとポートを入力します。認証要求の転送に使用する転送インターフェイスを選択します。同時接続の最大数を指定します。次に、アプライアンスから転送サーバへの接続に対して TLS を必須とするかどうかを設定します。使用する SASL メカニズムも、[プレーン（PLAIN）] と [ログイン（LOGIN）] から選択できます（使用できる場合）。この選択は、転送サーバごとに設定されます。

ステップ 7 変更を送信し、保存します。

ステップ 8 認証プロファイルの作成が完了すると、そのプロファイルをリスナーに対してイネーブルにできます。詳細については、リスナーでの SMTP 認証の有効化 （41 ページ）を参照してください。

LDAP を使用する SMTP 認証

LDAP ベースの SMTP 認証プロファイルを作成するには、SMTP 認証クエリを LDAP サーバ プロファイルと共に [システム管理（System Administration）] > [LDAP] ページであらかじめ作成しておく必要があります。このプロファイルを使用して SMTP 認証プロファイルを作成します。LDAP プロファイルの作成方法の詳細については、LDAP クエリについて （2 ページ）を参照してください。

手順

ステップ 1 [ネットワーク（Network）] > [SMTP認証（SMTP Authentication）] を選択します。

ステップ 2 [プロファイルを追加（Add Profile）] をクリックします。

ステップ 3 SMTP 認証プロファイルの一意の名前を入力します。

ステップ 4 [プロファイルタイプ（Profile Type）] で [LDAP] を選択します。

ステップ 5 [Next] をクリックします。

ステップ 6 この認証プロファイルに使用する LDAP クエリを選択します。

ステップ 7 デフォルトの暗号化方式をドロップダウン メニューから選択します。選択肢には、[SHA]、[Salted SHA]、[Crypt]、[Plain]、[MD5] があります。LDAP サーバによって暗号化後のパスフレーズの前に暗号化タイプが付加される場合は、[なし（None）] を選択してください。LDAP サーバによって暗号化タイプが別エンティティとして保存される場合は（たとえば OpenWave LDAP サーバ）、暗号化方式をメニューから選択してください。デフォルトの暗号化設定は、LDAP クエリにバインドが使用される場合は使用されません。

ステップ 8 [終了（Finish）] をクリックします。

ステップ 9 変更を送信し、保存します。

ステップ 10 認証プロファイルの作成が完了すると、そのプロファイルをリスナーに対してイネーブルにできます。詳細については、リスナーでの SMTP 認証の有効化 （41 ページ）を参照してください。

次のタスク

関連項目

- リスナーでの SMTP 認証の有効化 （41 ページ）

リスナーでの SMTP 認証の有効化

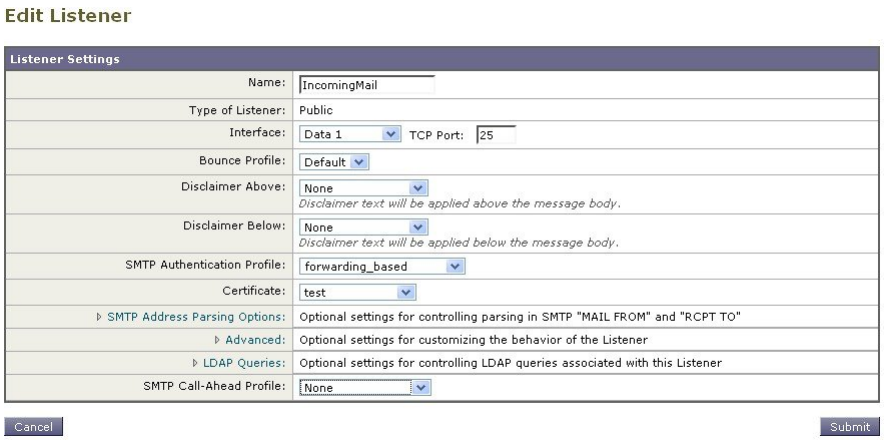
[ネットワーク（Network）] > [SMTP認証（SMTP Authentication）] ページで、実行する認証のタイプ（LDAP ベースまたは SMTP 転送ベース）を指定して SMTP 認証「プロファイル」を作成したら、[ネットワーク（Network）] > [リスナー（Listeners）] ページ（または **`listenerconfig`** コマンド）を使用して、このプロファイルをリスナーに関連付ける必要があります。

（注） 認証済みのユーザには、ユーザのその時点のメール フロー ポリシーの中で RELAY 接続動作が許可されます。

1 つのプロファイル内で複数の転送サーバを指定することもできます。SASL メカニズム CRAM-MD5 と DIGEST-MD5 は、アプライアンスと転送サーバの間ではサポートされません。

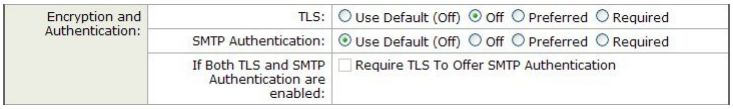
次の例では、リスナー「InboundMail」で SMTPAUTH プロファイルが使用されるように、[リスナーを編集（Edit Listener）] ページで設定しています。

図 *11 : SMTP* 認証プロファイルを *[*リスナーを編集（*Edit Listener*）*]* ページで選択する



プロファイルを使用するようにリスナーを設定したら、そのリスナーでの SMTP 認証を許可、禁止、または必須とするようにホスト アクセス テーブルのデフォルト設定を変更できます。

図 *12 :* メール フロー ポリシーでの *SMTP* 認証のイネーブル化



ケース	説明
1.	[SMTP認証（SMTP Authentication）] フィールドでは、リスナー レベルで SMTP 認証を制御します。[いいえ（No）] を選択した場合は、SMTP 認証に関する他の設定にかかわらず、このリスナーでは認証はイネーブルになりません。
2.	2 番めのプロンプト（[SMTP認証（SMTP Authentication）]）で [必須（Required）] を選択した場合は、AUTH キーワードが発行されるのは TLS がネゴシエートされた（クライアントが別の EHLO コマンドを発行した）後となります。

関連項目

- SMTP 認証と HAT ポリシーの設定 （43 ページ）
- HAT 遅延拒否 （43 ページ）

SMTP 認証と HAT ポリシーの設定

送信者は送信者グループとしてまとめられ、その後でSMTP認証ネゴシエーションが開始するので、ホスト アクセス テーブル（HAT）の設定には影響は及びません。リモート メール ホストが接続するときに、アプライアンスは初めにどの送信者グループが該当するかを特定して、その送信者グループのメール ポリシーを適用します。たとえば、リモート MTA「suspicious.com」が SUSPECTLIST という送信者グループに属している場合は、「suspicious.com」の SMTPAUTH ネゴシエーションの結果とは無関係に THROTTLE ポリシーが適用されます。

ただし、SMTPAUTH を使用して認証を受ける送信者の扱いは、「通常の」送信者とは異なります。SMTPAUTH セッションに成功した場合の接続動作は「RELAY」に変更されるので、実質的に受信者アクセス テーブル（RAT）と LDAPACCEPT はバイパスされます。その結果、送信者はメッセージをアプライアンス経由でリレーできます。したがって、適用されるレート制限やスロットリングがある場合は、引き続き有効になります。

HAT 遅延拒否

HAT 遅延拒否が設定済みのときは、HAT 送信者グループとメール フロー ポリシーの設定に基づいて本来ならばドロップされる接続も、認証に成功し、RELAY メール フロー ポリシーが許可されます。

メッセージ受信者レベルでHAT拒否を実行するかどうかを設定します。デフォルトでは、HATによって拒否された接続は SMTP カンバセーションの開始時にバナー メッセージをともなって終了されます。

HAT「拒否」設定で電子メールが拒否されると、AsyncOS ではSMTPカンバセーションの開始時ではなく、メッセージ受信者レベル（RCPT TO）で拒否を実行できます。この方法でメッセージを拒否することで、メッセージの拒否が遅延されメッセージがバウンスするため、AsyncOSは拒否されたメッセージに関するより詳細な情報を取得できます。たとえば、ブロックされたメッセージのアドレスおよび各受信者のアドレスからメールを表示できます。また、HAT 拒否の遅延によって、送信側 MTA が何度も再試行される可能性も小さくなります。

HAT 遅延拒否をイネーブルにすると、次の動作が発生します。

- MAIL FROM コマンドが許可されるが、メッセージ オブジェクトは作成されない。
- 電子メールの送信のためのアクセスが拒否されたというメッセージが表示され、すべての RCPT TO コマンドが拒否される。
- SMTP AUTH を使用して送信側 MTA が認証される場合、RELAY ポリシーが許可され、メールを通常どおりに送信できる。

遅延拒否を設定するには、CLI の `listenerconfig --> setup` コマンドを使用します。この動作は、デフォルトではディセーブルになっています。

次の表に、HAT の遅延拒否を設定する方法を説明します。

```
example.com> listenerconfig


Currently configured listeners:

1. listener1 (on main, 172.22.138.17) QMQP TCP Port 628 Private
```

```
2. listener2 (on main, 172.22.138.17) 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.


[]> setup

Enter the global limit for concurrent connections to be allowed across all listeners.

[300]>


[...]


By default HAT rejected connections will be closed with a banner
message at the start of the SMTP conversation. Would you like to do the rejection at the
message recipient level instead for more detailed logging of rejected mail?

[N]> y

Do you want to modify the SMTP RCPT TO reject response in this case?

[N]> y

Enter the SMTP code to use in the response. 550 is the standard code.

[550]> 551

Enter your custom SMTP response. Press Enter on a blank line to finish.

Sender rejected due to local mail policy.

Contact your mail admin for assistance.
```

クライアント証明書を使用した SMTP セッションの認証

E メール セキュリティ アプライアンスは、E メール セキュリティ アプライアンスとユーザのメール クライアント間の SMTP セッションを認証するためにクライアント証明書の使用をサポートします。

SMTP認証プロファイルを作成する場合は、証明書を確認するときに使用する証明書認証LDAPクエリを選択します。また、クライアント証明書が使用できなかった場合、Eメールセキュリティ アプライアンスがユーザ認証するための SMTP AUTH コマンドにフォールバックするかどうかを指定できます。

組織でユーザを認証するためにクライアント証明書を使用する場合、クライアント証明書を持たないユーザがユーザのデータが許可するように指定されている限りメールを送信できるかどうか判断するために、SMTP 認証クエリを使用できます。

発信 SMTP 認証

SMTP 認証は、発信メール リレーをユーザ名とパスフレーズを使用して検証するときにも使用できます。「発信」SMTP 認証プロファイルを作成してから、このプロファイルを全ドメインの SMTP ルートに関連付けます。メール配信試行のたびに、 アプライアンスは必要なクレデンシャルを使用してアップストリーム メール リレーにログインします。SMTP 認証は、認証プロトコルの PLAIN と LOGIN をサポートします。

手順

ステップ 1 送信 SMTP 認証プロファイルを作成します。

1. [ネットワーク（Network）] > [SMTP認証（SMTP Authentication）] を選択します。
2. [プロファイルを追加（Add Profile）] をクリックします。
3. SMTP 認証プロファイルの一意の名前を入力します。
4. [プロファイルタイプ（Profile Type）] で [送信（Outgoing）] を選択します。
5. [次へ（Next）] をクリックします。
6. 認証プロファイルの認証用ユーザ名とパスフレーズを入力します。
7. [終了（Finish）] をクリックします。

ステップ 2 ステップ 1 で作成した送信 SMTP 認証プロファイルを使用するように、SMTP ルートを設定します。

1. [ネットワーク（Network）] > [SMTPルート（SMTP Routes）] を選択します。
2. テーブルの [受信ドメイン（Receiving Domain）] カラムで、[その他のすべてのドメイン（All Other Domains）] リンクをクリックします。
3. SMTP ルートの宛先ホストの名前を [宛先ホスト（Destination Host）] に入力します。これは、発信メールの配信に使用される外部メール リレーのホスト名です。
4. 発信 SMTP 認証プロファイルをドロップダウン メニューから選択します。
5. 変更を送信し、保存します。

ロギングと SMTP 認証

SMTP 認証メカニズム（LDAP ベース、SMTP 転送サーバ ベース、または SMTP 発信）がアプライアンス上で設定されている場合は、以下のイベントがメール ログに記録されます。

- （情報）SMTP 認証成功：認証されたユーザと、使用されたメカニズムも記録されます。（プレーン テキストのパスフレーズが記録されることはありません）。
- （情報）SMTP 認証失敗：認証されたユーザと、使用されたメカニズムも記録されます。

- （警告）認証サーバに接続不可能：サーバ名とメカニズムも記録されます。
- （警告）タイムアウトイベント：転送サーバ（アップストリームの、インジェクションを行うアプライアンスと通信）が認証要求を待つ間にタイムアウトした場合。

ユーザの外部 LDAP 認証の設定

ネットワーク上のLDAPディレクトリを使用してユーザを認証するようにアプライアンスを設定できます。このように設定すると、ユーザが各自のLDAPユーザ名とパスフレーズを使用してログインできるようになります。LDAP サーバに対する認証クエリを設定したら、アプライアンスによる外部認証の使用をイネーブルにします（GUI の [システム管理（System Administration）] > [ユーザ（Users）] ページまたは CLI の **userconfig** コマンドを使用します）。

手順

ステップ 1 **ユーザ アカウントを検索するためのクエリーを作成します。**LDAP サーバ プロファイルで、LDAP ディレクトリ内のユーザ アカウントを検索するためのクエリを作成します。

ステップ 2 **グループ メンバーシップ クエリーを作成します。**ユーザが特定のディレクトリ グループのメンバーかどうかを判断するためのクエリを作成します。

ステップ 3 **LDAP サーバを使用するように外部認証をセットアップします。**この LDAP サーバをユーザ認証に使用するようにアプライアンスを設定し、ユーザ ロールを LDAP ディレクトリ内のグループに割り当てます。詳細については、「Distributing Administrative Tasks」の章の「Adding Users」を参照してください。

（注） [LDAP] ページの [クエリのテスト（Test Query）] ボタン（または **ldaptest** コマンド）を使用して、クエリから返される結果が期待したとおりであることを確認します。詳細については、LDAP クエリのテスト （19 ページ）を参照してください。

次のタスク

関連項目

- ユーザ アカウント クエリ （46 ページ）
- グループ メンバーシップ クエリ （47 ページ）

ユーザ アカウント クエリ

外部ユーザを認証するために、AsyncOS はクエリを使用してそのユーザのレコードを LDAP ディレクトリ内で検索し、ユーザのフル ネームが格納されている属性を見つけます。選択したサーバ タイプに応じて、AsyncOS によってデフォルト クエリーとデフォルト属性が入力されます。アカウントが失効しているユーザは拒否するようにアプライアンスを設定することもできます。それには、RFC 2307 で規定されている属性が LDAP ユーザ レコード内で定義されて

いる必要があります（shadowLastChange、shadowMax、および shadowExpire）。ユーザ レコードが存在するドメイン レベルのベース DN が必須です。

次の表に、AsyncOS がユーザ アカウントを Active Directory サーバ上で検索するときに使用されるデフォルトのクエリ文字列とユーザのフル ネーム属性を示します。

表 *7:* デフォルトのユーザ アカウント クエリ文字列と属性：*Active Directory*

サーバ タイプ（Server Type）	Active Directory
ベース DN（Base DN）	（ブランク）（ユーザ レコードを見つけるには具体的なベース DN を使用する必要があります）
クエリ文字列	(&(objectClass=user)(sAMAccountName={u}))
ユーザのフル ネームが格納されている属性（Attribute containing the user's full name）	displayName

次の表に、AsyncOS がユーザ アカウントを OpenLDAP サーバ上で検索するときに使用されるデフォルトのクエリ文字列とユーザのフル ネーム属性を示します。

表 *8:* デフォルトのユーザ アカウント クエリ文字列と属性：*OpenLDAP*

サーバ タイプ（Server Type）	OpenLDAP
ベース DN（Base DN）	（ブランク）（ユーザ レコードを見つけるには具体的なベース DN を使用する必要があります）
クエリ文字列	(&(objectClass=posixAccount)(uid={u}))
ユーザのフル ネームが格納されている属性（Attribute containing the user's full name）	gecos

グループ メンバーシップ クエリ

AsyncOS は、ユーザが特定のディレクトリ グループのメンバーかどうかを判断するという目的でもクエリを使用します。ディレクトリ グループ メンバーシップ内のメンバーシップによって、そのユーザのシステム内のアクセス許可が決まります。GUI の [システム管理（System Administration）]>[ユーザ（Users）] ページ（または CLI の userconfig）で外部認証をイネーブルにするときに、ユーザ ロールを LDAP ディレクトリ内のグループに割り当てます。ユーザ ロールによって、そのユーザがシステム内で持つアクセス許可が決まります。外部認証されたユーザの場合は、ロールは個々のユーザではなくディレクトリ グループに割り当てられます。たとえば、IT というディレクトリ グループ内のユーザに Administrator ロールを割り当て、Support というディレクトリ グループのユーザに Help Desk User ロールを割り当てます。

1 人のユーザが複数の LDAP グループに属しており、それぞれユーザ ロールが異なる場合は、最も限定的なロールのアクセス許可が AsyncOS によってそのユーザに付与されます。たとえば、ユーザが Operator 権限を持つグループと Help Desk User 権限を持つグループに属する場合、AsyncOS はユーザに Help Desk User ロールの権限を割り当てます。

グループ メンバーシップを問い合わせるための LDAP プロファイルを設定するときに、グループ レコードが格納されているディレクトリ レベルのベース DN を入力し、グループ メンバーのユーザ名が格納されている属性と、グループ名が格納されている属性を入力します。LDAP サーバ プロファイルに対して選択されたサーバ タイプに基づいて、ユーザ名とグループ名の属性のデフォルト値とデフォルト クエリ文字列が AsyncOS によって入力されます。

（注） Active Directory サーバの場合は、ユーザが特定のグループのメンバーかどうかを判断するためのデフォルトのクエリ文字列は (&(objectClass=group)(member={u})) です。ただし、使用する LDAP スキーマにおいて、「memberof」のリストでユーザ名ではなく識別名が使用されている場合は、{dn} を {u} の代わりに使用できます。

次の表に、AsyncOS が Active Directory サーバ上でグループ メンバーシップ情報を検索するときに使用されるデフォルトのクエリ文字列と属性を示します。

表 *9:* デフォルトのグループ メンバーシップ クエリ文字列と属性：*Active Directory*

サーバ タイプ（Server Type）	Active Directory
ベース DN（Base DN）	（ブランク）（グループ レコードを見つけるには具体的なベース DN を使用する必要があります）
ユーザが特定のグループのメンバーかどうかを判断するためのクエリー文字列	(&(objectClass=group)(member={u})) （注） 使用する LDAP スキーマにおいて memberOf リストの中でユーザ名ではなく識別名が使用されている場合は、{u} の代わりに {dn} を使用できます。
各メンバーのユーザ名（またはそのユーザのレコードの DN）が格納されている属性	member
グループ名が格納されている属性	cn

次の表に、AsyncOS が OpenLDAP サーバ上でグループ メンバーシップ情報を検索するときに使用されるデフォルトのクエリ文字列と属性を示します。

表 *10 :* デフォルトのグループ メンバーシップ クエリ文字列と属性：*OpenLDAP*

サーバ タイプ（Server Type）	OpenLDAP
ベース DN（Base DN）	（ブランク）（グループ レコードを見つけるには具体的なベース DN を使用する必要があります）
ユーザが特定のグループのメンバーかどうかを判断するためのクエリー文字列	(&(objectClass=posixGroup)(memberUid={u}))
各メンバーのユーザ名（またはそのユーザのレコードのDN）が格納されている属性	memberUid
グループ名が格納されている属性	cn

スパム隔離機能へのエンド ユーザ認証

スパム隔離へのエンドユーザ認証のクエリとは、ユーザがスパム隔離機能にログインするときにユーザを検証するためのクエリです。トークン {u} は、ユーザを示します（ユーザのログイン名を表します）。トークン {a} は、ユーザの電子メール アドレスを示します。LDAP クエリによって「SMTP:」が電子メールアドレスから除去されることはありません。ただし、AsyncOS はこの部分をアドレスから除去します。

スパム隔離機能のエンドユーザ アクセス検証に LDAP クエリを使用するには、[有効なクエリとして指定する（Designate as the active query）] チェックボックスをオンにしてください。すでにアクティブなクエリがある場合、そのクエリはディセーブルになります。[システム管理（System Administration）]>[LDAP] ページを開いたときに、アクティブなクエリの横にアスタリスク（*）が表示されます。

サーバ タイプに基づいて、次のデフォルト クエリ文字列がエンドユーザ認証クエリに使用されます。

- Active Directory：(sAMAccountName={u})
- **OpenLDAP**：(uid={u})
- 不明またはそれ以外（Unknown or Other）：（ブランク）

デフォルトでは、プライマリ メール属性は Active Directory サーバの場合は proxyAddresses、OpenLDAP サーバの場合は mail です。独自のクエリとメール属性を入力できます。クエリを CLI で作成するには、ldapconfig コマンドの isqauth サブコマンドを使用します。

（注） ユーザのログイン時に各自のメールアドレス全体を入力させる場合は、(mail=smtp:{a}) というクエリ文字列を使用します。

関連項目

- Active Directory エンドユーザ認証の設定例 （50 ページ）
- OpenLDAP エイリアス統合の設定例 （52 ページ）
- スパム隔離へのエンドユーザ アクセスの設定

Active Directory エンドユーザ認証の設定例

ここでは、Active Directory サーバとエンドユーザ認証クエリの設定の例を示します。この例では、Active Directory サーバに対してパスフレーズ認証を使用し、メール属性は mail と proxyAddresses を使用し、Active Directory サーバに対するエンドユーザ認証にはデフォルトのクエリ文字列を使用します。

表 *11 : LDAP* サーバとスパム隔離へのエンドユーザ認証の設定例：*Active Directory*

認証方式	**パスフレーズを使用（検索用にバインドするための低特権のユーザを作成するか、匿名検索を設定する必要があります）**
サーバ タイプ（Server Type）	Active Directory
[ポート（Port）]	3268
ベース DN（Base DN）	（ブランク）
接続プロトコル	（ブランク）
クエリ文字列	(sAMAccountName={u})
メール属性	mail,proxyAddresses

OpenLDAP エンドユーザ認証の設定の例

ここでは、OpenLDAP サーバとエンドユーザ認証クエリの設定の例を示します。この例では、OpenLDAP サーバに対して匿名認証を使用し、メール属性は mail と mailLocalAddress を使用し、OpenLDAP サーバに対するエンドユーザ認証にはデフォルトのクエリ文字列を使用します。

表 *12 : LDAP* サーバとスパム隔離へのエンドユーザ認証の設定例：*OpenLDAP*

認証方式	**匿名（Anonymous）**
サーバ タイプ（Server Type）	OpenLDAP
[ポート（Port）]	389

認証方式	匿名（Anonymous）
ベース DN（Base DN）	（ブランク）（古いスキーマでは具体的なベース DN の使用が要求されることがあります）
接続プロトコル	（ブランク）
クエリ文字列	(uid={u})
メール属性	mail,mailLocalAddress

スパム隔離のエイリアス統合クエリ

スパム通知を使用する場合は、スパム隔離のエイリアス統合クエリを使用して電子メールエイリアスを1つにまとめると、受信者がエイリアスごとに隔離通知を受け取ることはなくなります。たとえば、ある受信者がメール アドレス john@example.com、jsmith@example.com、および john.smith@example.com のメールを受け取るとします。エイリアス統合を使用すると、受信者が受け取るスパム通知は1通だけとなります。送信先は、このユーザのエイリアスすべてに送信されるメッセージのプライマリ電子メールアドレスとして選択されたアドレスです。

メッセージを統合してプライマリ電子メールアドレスに送信するには、受信者の代替電子メールエイリアスを検索するためのクエリを作成してから、受信者のプライマリ電子メールアドレスの属性を [メール属性（Email Attribute）] フィールドに入力します。

スパム隔離機能のスパム通知に LDAP クエリを使用するには、[有効なクエリとして指定する（Designate as the active query）] チェックボックスをオンにしてください。すでにアクティブなクエリがある場合、そのクエリはディセーブルになります。[システム管理（System Administration）] > [LDAP] ページを開いたときに、アクティブなクエリの横にアスタリスク（*）が表示されます。

Active Directory サーバの場合は、デフォルトのクエリ文字列は (|(proxyAddresses={a})(proxyAddresses=smtp:{a})) で、デフォルトのメール属性は mail です。OpenLDAP サーバの場合は、デフォルトのクエリ文字列は (mail={a}) で、デフォルトのメール属性は mail です。独自のクエリとメール属性を定義することもできます。属性が複数の場合は、カンマで区切ります。入力する電子メール属性が複数ある場合は、最初の電子メール属性として、変動する可能性のある値を複数持つ属性（たとえば proxyAddresses）ではなく、値を1つだけ使用する一意の属性（たとえば mail）を入力することを推奨します。

クエリを CLI で作成するには、ldapconfig コマンドの isqalias サブコマンドを使用します。

関連項目

- Active Directory エイリアス統合の設定例 （52 ページ）
- OpenLDAP エイリアス統合の設定例 （52 ページ）

Active Directory エイリアス統合の設定例

ここでは、Active Directory サーバとエイリアス統合クエリの設定の例を示します。この例では、Active Directory サーバに対して匿名認証を使用し、Active Directory サーバに対するエイリアス統合用のクエリ文字列を指定し、メール属性は mail を使用します。

表 *13 : LDAP* サーバとスパム隔離エイリアス統合の設定例：*Active Directory*

認証方式	**匿名（Anonymous）**
サーバ タイプ（Server Type）	Active Directory
[ポート（Port）]	3268
ベース DN（Base DN）	（ブランク）
接続プロトコル	SSL を使用する（Use SSL）

クエリ文字列	`(`
	`|(mail={a})(mail=smtp:{a})`
	`)`

メール属性	メール アドレス

（注） この例は、説明のみを目的としています。クエリおよび OU、またはツリー設定は、環境と設定によって異なる場合があります。

OpenLDAP エイリアス統合の設定例

ここでは、OpenLDAP サーバとエイリアス統合クエリの設定の例を示します。この例では、OpenLDAP サーバに対して匿名認証を使用し、OpenLDAP サーバに対するエイリアス統合用のクエリ文字列を指定し、メール属性は mail を使用します。

表 *14 : LDAP* サーバとスパム隔離エイリアス統合の設定例：*OpenLDAP*

認証方式	**匿名（Anonymous）**
サーバ タイプ（Server Type）	OpenLDAP
[ポート（Port）]	389
ベース DN（Base DN）	（ブランク）（古いスキーマでは具体的なベース DN の使用が要求されることがあります）
接続プロトコル	SSL を使用する（Use SSL）

認証方式	匿名（Anonymous）
クエリ文字列	(mail={a})
メール属性	メール アドレス

（注） この例は、説明のみを目的としています。クエリおよびOU、またはツリー設定は、環境と設定によって異なる場合があります。

ユーザ識別名の設定の例

ここでは、Active Directoryサーバとエンドユーザ識別名クエリの設定の例を示します。この例では、Active Directoryサーバに対して匿名認証を使用し、Active Directoryサーバに対するユーザの識別名検索用のクエリ文字列を指定ます。

表 *15 : LDAP* サーバとスパム隔離エイリアス統合の設定例：*Active Directory*

認証方式	匿名（Anonymous）
サーバ タイプ（Server Type）	Active Directory
[ポート（Port）]	3268
ベース DN（Base DN）	（ブランク）
接続プロトコル	SSL を使用する（Use SSL）
クエリ文字列	`(proxyAddresses=smtp:{a})`

（注） この例は、説明のみを目的としています。クエリおよびOU、またはツリー設定は、環境と設定によって異なる場合があります。

AsyncOS を複数の LDAP サーバと連携させるための設定

LDAPプロファイルを設定するときに、アプライアンスからの接続先となる複数のLDAPサーバをリストとして設定できます。複数のLDAPサーバを使用するには、LDAPサーバに格納されている情報が同一になるように設定する必要があります。また、構造も同一で、使用する認証情報も同一でなければなりません（レコードを統合できる製品がサードパーティから提供されています）。

冗長化した複数のLDAPサーバに接続するようにアプライアンスを設定すると、LDAPのフェールオーバーまたはロード バランシングを設定できます。

複数の LDAP サーバを使用すると、次のことが可能になります。

- **フェールオーバー**。フェールオーバーのためのLDAPプロファイルを設定しておくと、アプライアンスが最初の LDAP サーバに接続できなくなったときに、リスト内の次の LDAP サーバへのフェールオーバーが行われます。
- **ロード バランシング**。ロード バランシングのための LDAP プロファイルを設定しておくと、アプライアンスがLDAPクエリを実行するときに、アプライアンスからの接続はリスト内の LDAP サーバに分散されます。

冗長 LDAP サーバを設定するには、[システム管理（System Administration）] > [LDAP] ページまたは CLI の ldapconfig コマンドを使用します。

Office 365-LDAP コネクタを使用した、受信者検証の実行とグループ クエリの解決

Office 365-LDAP コネクタ ツールを使用すると、Azure Active Directory（AD）からユーザ詳細およびグループ情報を取得し、シスコのクラウド環境に設定したLDAPサーバーに保存できます。インスタンスのLDAPプロファイルに向けて設定したアクションを使用して、LDAP サーバーに対して LDAP 受信者検証とグループ クエリを実行できます。

始める前に

Cisco Connection Online ID（CCO ID）と契約番号を使用して Cisco TAC チケットを開き、インスタンスで Office 365-LDAP コネクタ ツールを有効にします。詳細については、Cisco TAC にお問い合わせください。

（注） 手順のステップ 1 および 2 を実行する際は、『*Azure to LDAP Connector Guide*』（https://ces.readme.io/v1.0/docs/azure-to-ldap-connector）を参照してください。

手順

ステップ 1 Azure管理ポータル内でx509証明書を作成し、プライベート キーを生成して、Office 365-LDAP コネクタ ツールが AD にアクセスすることを許可します。

ステップ 2 Azure API を設定して、AD のすべてのユーザ グループおよびユーザ ディレクトリ データに読み取りアクセス許可を与えます。

ステップ2の指示を完了すると、Azure ADのすべてのユーザ詳細とグループ情報がLDAPサーバにコピーされます。シスコからの歓迎レターと、インスタンスでLDAPプロファイルを設定するための LDAP サーバ設定が届きます。

（注） LDAP サーバで、各組織は個別の組織ユニット（OU）として分類されています。

ステップ 3 自己署名の証明書を作成して、インスタンスでメールボックスの自動修復（MAR）のメールボックス設定を構成します。詳細については、Cisco TechZone の記事（https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/213842-azure-ad-configuration-script-for-cisco.html）を参照してください。

ステップ 4 以下のステップを実行して、新しいLDAPプロファイルを設定するか、インスタンスの既存のLDAP プロファイルを再設定します。

a) [システム管理（System Administration）] > [LDAP] ページに移動します。

b) [LDAPサーバプロファイルの追加（Add LDAP Server Profile）] をクリックして新しいLDAP プロファイルを設定するか、既存の LDAP サーバプロファイル リンクをクリックして既存の LDAP プロファイルを再設定します。

c) 歓迎レターで受け取った以下の LDAP サーバ設定を設定します。

- サーバIP（Server IP）
- ベース DN（Base DN）
- バインド DN（Bind DN）
- バインド パスワード（Bind Password）
- サーバ タイプ（Server Type）：OpenLDAP
- UseSSL: Yes（ポート 636）
- 受け入れクエリ（Accept Query）：(mail={a})
- グループ クエリ（Group Query）：(&(objectClass=posixGroup)(cn=[g])(memberUid={a}))

d) [受け入れクエリ（Accept Query）] と [グループクエリ（Group Query）] をチェックし、有効および無効なメール アドレスを使用して両方のクエリをテストします。

e) 変更を送信し、保存します。

f) [ネットワーク（Network）] > [リスナー（Listeners）] ページに移動し、パブリック リスナー名のリンクをクリックします。

g) [LDAPクエリ（LDAP Queries）] をクリックし、設定した受け入れクエリとグループクエリを選択します。

h) 変更を送信し、保存します。

i) [メールポリシー（Mail Policies）] > [受信者アクセステーブル（RAT）（Recipient Access Table (RAT)）] ページに移動し、受信者のアドレスのリンクをクリックします。

j) 特定の受信者に対して、アプライアンスで LDAP 受け入れクエリがバイパスされないようにするには、その受信者の [LDAP受け入れクエリのバイパス（Bypass LDAP Accept Queries）] の選択を解除します。

k) 変更を送信し、保存します。

ステップ 5 24 時間後に Cisco TAC チケットを表示し、すべてのユーザ詳細とグループ情報が Azure AD から LDAP サーバにコピーされたかどうかを確認します。

24 時間が経過してもすべてのユーザ詳細とグループ情報が Azure AD から LDAP サーバにコピーされていない場合は、Cisco TAC に問い合わせてテクニカル サポートを受けてください。

サーバとクエリのテスト

[Add（または Edit）LDAP Server Profile] ページの [テストサーバ（Test Server(s)）] ボタン（または CLI の **test** サブコマンド）を使用して、LDAP サーバへの接続をテストします。複数の LDAP サーバを使用する場合は、各サーバのテストが実行されて、各サーバの結果が個別に表示されます。各 LDAP サーバでのクエリのテストも実行されて、結果が個別に表示されます。

関連項目

- フェールオーバー （56 ページ）
- ロード バランシング （57 ページ）

フェールオーバー

LDAP クエリが確実に解決されるようにするには、フェールオーバーのための LDAP プロファイルを設定します。LDAP サーバへの接続に失敗した場合、または問い合わせで特定のエラーコード（利用不可やビジーなど）が返される場合、アプライアンスはリストで指定されている次の LDAP サーバへの問い合わせを試行します。

アプライアンスは、LDAP サーバ リスト内の最初のサーバへの接続を、所定の時間が経過するまで試行します。アプライアンスがリストの最初の LDAP サーバに接続できない場合、または問い合わせで特定のエラーコード（利用不可やビジーなど）が返される場合、アプライアンスはリストの次の LDAP サーバへの接続を試行します。デフォルトでは、アプライアンスは常にリスト内の最初のサーバへの接続を試行し、それ以降の各サーバへの接続を、リスト内で指定されている順に試行します。アプライアンスが確実にプライマリの LDAP サーバにデフォルトで接続するようにするには、そのサーバが LDAP サーバ リストの先頭に入力されていることを確認してください。

アプライアンスが 2 番め以降の LDAP サーバに接続した場合は、タイムアウトの時間に達するまで、そのサーバに接続したままになります。タイムアウトの時間に達すると、リスト内の最初のサーバへの再接続が試行されます。

（注） 指定された LDAP サーバを問い合わせる試行のみがフェールオーバーします。指定された LDAP サーバに関連付けられた参照サーバまたは継続サーバを問い合わせる試行はフェールオーバーしません。

関連項目

- LDAP フェールオーバーのためのアプライアンスの設定 （57 ページ）

LDAP フェールオーバーのためのアプライアンスの設定

LDAP フェールオーバーを行うようにアプライアンスを設定するには、GUI で以下の手順を実行します。

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] ページで、編集する LDAP サーバ プロファイルを選択します。

ステップ 2 LDAP サーバ プロファイルから、次の項目を設定します。

ケース	説明
1	LDAP サーバの一覧を表示します。
2	最大接続数を設定します。

ステップ 3 他の LDAP 設定を指定して変更を確定します。

ロード バランシング

LDAP 接続をグループ内の LDAP サーバ間に分散させるには、ロード バランシングのための LDAP プロファイルを設定します。

ロード バランシングのための LDAP プロファイルを設定しておくと、アプライアンスからの接続はリスト内の LDAP サーバに分散されます。接続に失敗したときやタイムアウトしたときは、アプライアンスは使用可能な LDAP サーバを判断して、使用可能なサーバに再接続します。アプライアンスは、管理者が設定した最大同時接続数に基づいて、同時に確立する接続の数を決定します。

リストで指定された LDAP サーバの 1 つが応答しなくなった場合は、アプライアンスからの接続の負荷は残りの LDAP サーバに分散されます。

関連項目

- ロード バランシングのためのアプライアンスの設定 （58 ページ）

ロード バランシングのためのアプライアンスの設定

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] ページで、編集する LDAP サーバ プロファイルを選択します。

ステップ 2 LDAP サーバ プロファイルから、次の項目を設定します。

ケース	説明
1	LDAP サーバの一覧を表示します。
2	最大接続数を設定します。

ステップ 3 他の LDAP 設定を指定して変更を確定します。