CHAPTER 10

LDAP クエリー

この章は、次の内容で構成されています。

概要

エンドユーザのパスワードおよび電子メール エイリアスを企業の LDAP ディレクトリ（Microsoft Active Directory、SunONE Directory Server、OpenLDAP ディレクトリなど）で維持する場合、LDAP ディレクトリを使用すると、Cisco IronPort スパム検疫にアクセスするユーザを認証できます。ユーザが Cisco IronPort スパム検疫の Web UI にログインするときに、LDAP サーバがログイン名とパスワードを検証し、AsyncOS が対応する電子メール エイリアスのリストを取得します。ユーザのいずれかの電子メール エイリアスに送信された検疫済みメッセージは、アプライアンスが上書きしていない限り、Cisco IronPort スパム検疫で表示できます。

Cisco IronPort スパム検疫との連携に必要な LDAP の設定

Cisco IronPort 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、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を設定する必要があります。

ステップ 1　LDAP サーバ プロファイルを設定します。

サーバ プロファイルの内容は、AsyncOS から LDAP サーバに接続するための、次のような情報です。

- サーバ名とポート
- ベース DN
- サーバにバインディングするための認証要件

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 プロファイルの作成」（P.10-3）を参照してください。

LDAP サーバ プロファイルを作成するときに、複数の LDAP サーバに接続するように AsyncOS を設定できます。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」（P.10-17）を参照してください。

ステップ 2　LDAP クエリーを設定します。

LDAP サーバ プロファイル用に生成されたデフォルトのスパム検疫クエリーを使用することも、特定の LDAP 実装およびスキーマに合わせてカスタマイズした独自のクエリーを作成することもできます。次に、スパム通知、および検疫へのエンドユーザ アクセス検証に使用するアクティブ クエリーを指定します。

クエリーの詳細については、「LDAP クエリーの設定」（P.10-6）を参照してください。

ステップ 3　Cisco IronPort スパム検疫に対して、LDAP エンドユーザ アクセスおよびスパム通知をイネーブルにします。

エンドユーザが、自分の検疫エリアのメッセージを表示および管理できるように、Cisco IronPort スパム検疫への LDAP エンドユーザ アクセスをイネーブルにします。ユーザが複数の通知を受信しないように、スパム通知のエイリアス統合をイネーブルにすることもできます。

詳細については、「IronPort スパム検疫の設定」（P.7-3）を参照してください。

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 を設定した場合は、LDAP サーバに関する情報を保存するために、LDAP サーバ プロファイルを作成します。

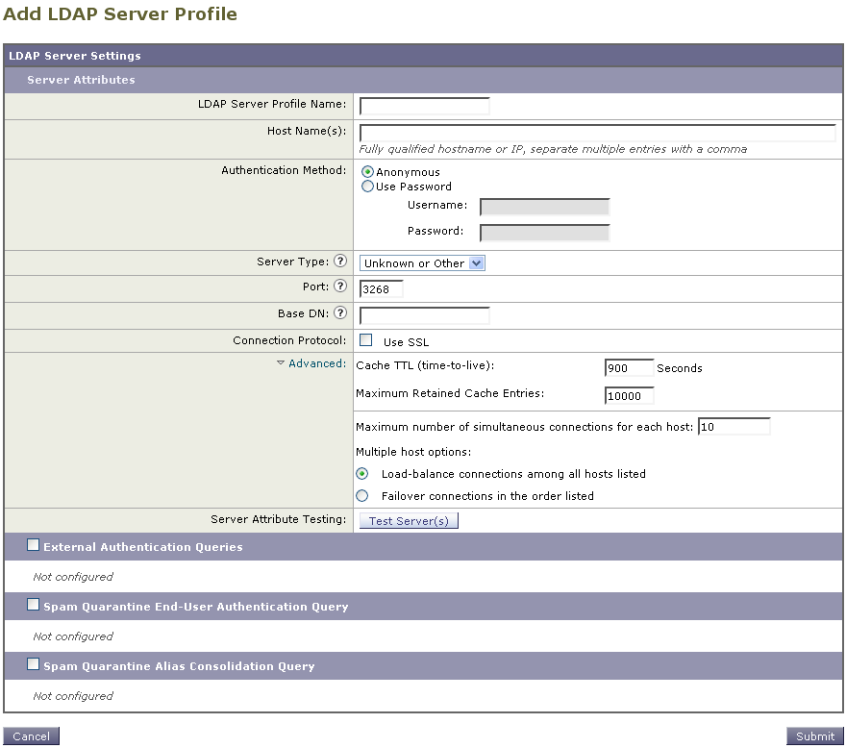
LDAP サーバ プロファイルを作成するには、次の手順を実行します。

ステップ 1　メイン Security Management アプライアンスで、[Management Appliance] > [System Administration] > [LDAP] を選択します。

ステップ 2　[Add LDAP Server Profile] をクリックします。

[Add LDAP Server Profile] ページが表示されます。

図 10-1　　LDAP サーバ プロファイルの設定



ステップ 3　[LDAP Server Profile Name] テキスト フィールドに、サーバ プロファイルの名前を入力します。

ステップ 4　[Host Name(s)] テキスト フィールドに、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」（P.10-17）を参照してください。

ステップ 5　認証方式を選択します。匿名認証を使用することも、ユーザ名とパスワードを指定することもできます。

（注）　レポートにクライアント IP アドレスではなくクライアント ユーザ ID を表示するには、LDAP 認証を設定する必要があります。LDAP 認証を使用しない場合、システムでは IP アドレスによるユーザの参照のみができます。[Use Password] オプション ボタンを選択して、ユーザ名とパスワードを入力します。[Internal Users Summary] ページにユーザ名が表示されます。

ステップ 6　LDAP サーバ タイプを [Active Directory]、[OpenLDAP]、[Unknown or Other] から選択します。

ステップ 7　ポート番号を入力します。

デフォルト ポートは 3268 です。これは、マルチサーバ環境でグローバル カタログにアクセスするための Active Directory のデフォルト ポートです。

ステップ 8　LDAP サーバのベース DN（識別名）を入力します。

ユーザ名とパスワードで認証を行う場合、ユーザ名にはパスワードが含まれているエントリの完全 DN が含まれている必要があります。たとえば、電子メール アドレスが joe@example.com というユーザがマーケティング グループのユーザだとします。このユーザのエントリは、次のようなエントリになります。

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

ステップ 9　[Advanced] の下で、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 10　キャッシュ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 11　保持するキャッシュ エントリの最大数を入力します。

ステップ 12　同時接続の最大数を入力します。

ロード バランシングを行うように LDAP サーバ プロファイルを設定した場合、リストで指定された LDAP サーバ間でこれらの接続が分散されます。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。詳細については、「ロード バランシング」（P.10-19）を参照してください。

（注） 同時接続の最大数には、LDAP クエリーに使用される LDAP 接続が含まれます。ただし、Cisco IronPort スパム検疫に対して LDAP 認証をイネーブルにした場合、アプライアンスによってエンドユーザ検疫用に 20 の追加接続が許可され、合計 30 の接続が許可されます。

ステップ 13　サーバへの接続をテストするために、[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 [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」（P.10-6）を参照してください。

ステップ 14　スパム検疫クエリーを作成します。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。

ユーザがエンドユーザ検疫にログインするときにそのユーザを検証する、検疫エンドユーザ認証クエリーを設定できます。エンドユーザが電子メール エイリアスごとに検疫通知を受信しないように、エイリアス統合クエリーを設定できます。これらのクエリーを使用するには、[Designate as the active query] チェックボックスをオンにします。詳細については、「LDAP クエリーの設定」（P.10-6）を参照してください。

ステップ 15　[Test Query] ボタンをクリックして、スパム検疫クエリーをテストします。

テスト パラメータを入力して [Run Test] をクリックします。テストの結果が [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、[Update] をクリックします。

（注） 空パスワード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、パスワード フィールドが空でもクエリーのテストは合格となります。

ステップ 16　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

Windows 2000 では、Active Directory サーバ設定で TLS を介した認証が許可されません。これは、Active Directory の既知の問題です。Active Directory と Windows 2003 の組み合わせでは、TLS 認証が機能します。

（注）　サーバ設定の数に制限はありませんが、サーバごとに設定できるエンドユーザ認証クエリー、およびエイリアス統合クエリーはそれぞれ 1 つだけです。

LDAP サーバのテスト

[Add/Edit LDAP Server Profile] ページの [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 サーバを設定した場合は、AsyncOS によって各サーバがテストされ、結果が個別に表示されます。

LDAP クエリーの設定

次のセクションで、Cisco IronPort スパム検疫クエリーのタイプごとに、デフォルトのクエリー文字列と設定の詳細を示します。

- **スパム検疫へのエンドユーザ認証のクエリー。**詳細については、「スパム検疫へのエンドユーザ認証のクエリー」（P.10-8）を参照してください。
- **スパム検疫のエイリアス統合のクエリー。**詳細については、「スパム検疫のエイリアス統合のクエリー」（P.10-10）を参照してください。

検疫機能のエンドユーザ アクセス検証またはスパム通知に LDAP クエリーを使用するには、[Designate as the active query] チェックボックスをオンにします。検疫アクセスを制御するエンドユーザ認証クエリーを 1 つと、スパム通知用のエイリアス統合クエリーを 1 つ指定できます。既存のすべてのアクティブ クエリーはディセーブルになります。Security Management アプライアンスで [Management Appliance] > [System Administration] > [LDAP] ページを選択すると、アクティブ クエリーの横にアスタリスク（*）が表示されます。

ドメインベースのクエリーまたはチェーン クエリーも、アクティブなエンドユーザ アクセス クエリーまたはスパム通知クエリーとして指定できます。詳細については、「ドメインベース クエリー」（P.10-12）および「チェーン クエ

リー」（P.10-14）を参照してください。

（注）　[LDAP] ページの [Test Query] ボタン（または **ldaptest** コマンド）を使用して、クエリー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。

LDAP クエリーの構文

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

クエリー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ーは、**maillocaladdress** と入力したときとは異なります。

トークン

次のトークンを LDAP クエリー内で使用できます。

- {a} ユーザ名 @ ドメイン名
- {d} ドメイン
- {dn} 識別名
- {g} グループ名
- {u} ユーザ名
- {f} MAILFROM: 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ーは、**(|(mail={a})(proxyAddresses=smtp:{a}))** になります。

（注）　作成したクエリーは、[LDAP] ページの [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 クエリーのテスト」（P.10-11）を参照してください。

スパム検疫へのエンドユーザ認証のクエリー

エンドユーザ認証のクエリーとは、ユーザが Cisco IronPort スパム検疫にログインするときにユーザを検証するためのクエリーです。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 クエリーによって「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。

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

- **Active Directory :** `(sAMAccountName={u})`
- **OpenLDAP :** `(uid={u})`
- **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 **mail** です。独自のクエリーとメール属性を入力できます。クエリーを 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電子メール アドレス全体を入力させる場合は、`(mail=smtp:{a})` というクエリー文字列を使用します。

Active Directory エンドユーザ認証の設定の例

ここでは、Active Directory サーバとエンドユーザ認証クエリー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ワード認証を使用し、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ー文字列を使用し、メール属性は `mail` と `proxyAddresses` を使用します。

表 10-1　LDAP サーバとスパム検疫へのエンドユーザ認証の設定例：Active Directory

認証方式	パスワードを使用 （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	Active Directory
ポート	3268
ベース DN	（ブランク）
接続プロトコル	（ブランク）
クエリー文字列	`(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ー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 サーバに対するエンドユーザ認証にはデフォルトのクエリー文字列を使用し、メール属性は `mail` と `mailLocalAddress` を使用します。

表 10-2　LDAP サーバとスパム検疫へのエンドユーザ認証の設定例：OpenLDAP

認証方式	匿名
サーバ タイプ	OpenLDAP
ポート	389
ベース 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）
クエリー文字列	`(uid={u})`
メール属性	`mail,mailLocalAddress`

スパム検疫のエイリアス統合のクエリー

スパム通知を使用する場合は、スパム検疫のエイリアス統合クエリー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検疫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 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 メール アドレスに送信するには、受信者の代替メール アドレスを検索するためのクエリーを作成してから、受信者のプライマリ メール アドレスを [Email Attribute] フィールドに入力します。

Active Directory サーバの場合は、デフォルトのクエリー文字列は `(|(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ー文字列は `(mail={a})` で、デフォルトのメール属性は `mail` です。独自のクエリー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。入力するメール属性が複数ある場合は、最初のメール属性として、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。

クエリーを 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。

Active Directory エイリアス統合の設定の例

ここでは、Active Directory サーバとエイリアス統合クエリー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ー文字列を指定し、メール属性は `mail` を使用します。

表 10-3　LDAP サーバとスパム検疫のエイリアス統合の設定例：Active Directory

認証方式	匿名
サーバ タイプ	Active Directory
ポート	3268
ベース DN	（ブランク）

表 10-3　LDAP サーバとスパム検疫のエイリアス統合の設定例：Active Directory（続き）

接続プロトコル	Use SSL
クエリー文字列	(|(mail={a})(mail=smtp:{a}))
メール属性	mail

OpenLDAP エイリアス統合の設定の例

ここでは、OpenLDAP サーバとエイリアス統合クエリー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ー文字列を指定し、メール属性は mail を使用します。

表 10-4　LDAP サーバとスパム検疫のエイリアス統合の設定例：OpenLDAP

認証方式	**匿名**
サーバ タイプ	OpenLDAP
ポート	389
ベース 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	Use SSL
クエリー文字列	(mail={a}))
メール属性	mail

LDAP クエリーのテスト

[Add/Edit LDAP Server Profile] ページの [Test Query] ボタン（または CLI の ldaptest コマンドを使用して）、クエリーをテストします。クエリー接続テストの段階ごとに、詳細が表示されます。たとえば、SMTP 認証の最初の段階が成功したか、失敗したか、BIND 照合結果として true と false のどちらが返されたかが表示されます。

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.isqalias foo@cisco.com
```

クエリー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、メール属性に `mailLocalAddress` と入力したときに実行されるクエリーは、`maillocaladdress` と入力したときとは異なります。

クエリーをテストするには、テスト パラメータを入力して、[Run Test] をクリックします。[Test Connection] フィールドに結果が表示されます。エンドユーザ認証クエリーが成功すると、「Success: Action: match positive」という結果が表示されます。エイリアス統合クエリーの場合は、統合されたスパム通知の電子メール アドレスと共に、「Success: Action: alias consolidation」という結果が表示されます。クエリーが失敗すると、一致する LDAP レコードが見つからない、一致したレコードにメール属性が含まれていないなど、失敗の原因が表示されます。複数の LDAP サーバを使用している場合、Cisco IronPort アプライアンスは、LDAP サーバごとにクエリーをテストします。

ドメインベース クエリー

ドメインベース クエリーとは、LDAP クエリーをタイプ別にグループ化し、ドメインに関連付けたものです。ドメインベース クエリーが使用されるのは、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、エンドユーザ検疫アクセスのクエリーをすべての LDAP サーバに対して実行する必要がある場合です。たとえば、Bigfish という企業がドメイン Bigfish.com、Redfish.com、および Bluefish.com を所有し、各ドメインに関連付けられている従業員に対して異なる LDAP サーバを使用しているとします。Bigfish は、ドメインベース クエリーを使用して、3 つのドメインすべての LDAP ディレクトリに対してエンドユーザを認証できます。

ドメインベース クエリーを使用してエンドユーザ アクセスまたは Cisco IronPort スパム検疫の通知を制御するには、次の手順を実行します。

ステップ 1　ドメインベース クエリーで使用するドメインごとに 1 つずつ、LDAP サーバ プロファイルを作成します。各サーバ プロファイルに、ドメインベース クエリーで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 プロファイルの作成」（P.10-3）を参照してください。

ステップ 2　ドメインベース クエリーを作成します。ドメインベース クエリーを作成するときに、各サーバ プロファイルからクエリーを選択し、ドメインベース クエリーを Cisco IronPort スパム検疫のアクティブ クエリーとして指定します。クエリーの作成方法の詳細については、「ドメインベース クエリーの作成」（P.10-13）を参照してください。

ステップ 3　Cisco IronPort スパム検疫に対して、エンドユーザ アクセスまたはスパム通知をイネーブルにします。詳細については、「IronPort スパム検疫の設定」（P.7-3）を参照してください。

ドメインベース クエリーの作成

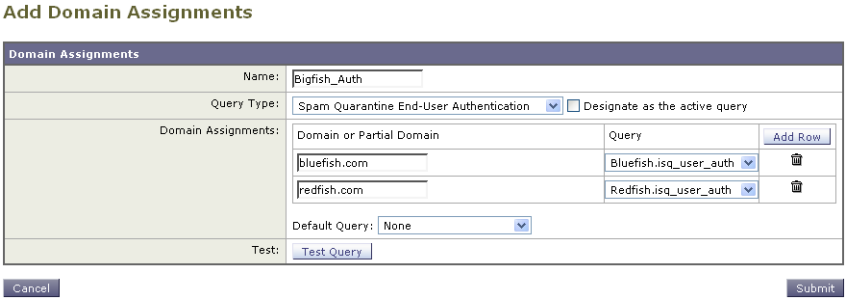
Security Management アプライアンスでドメインベース クエリーを作成するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [LDAP] を選択します。

ステップ 2　[LDAP] ページで、[Advanced] をクリックします。

[Add Domain Assignments] ページが表示されます。

図 10-2　　ドメインベース クエリーの設定



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　クエリーのタイプを選択します。

（注）　ドメインベース クエリーを作成するときは、クエリーのタイプを 1 つ指定します。クエリーのタイプを選択すると、該当するクエリーが LDAP サーバ プロファイルからクエリー フィールド ドロップダウン リストに設定されます。

ステップ 5　[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　行を追加して、ドメインベース クエリーのドメインごとにクエリーを選択します。

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

ステップ 9　[Test Query] ボタンをクリックし、[Test Parameters] フィールドにテストするユーザのログインとパスワード、または電子メール アドレスを入力して、クエリーをテストします。[Connection Status] フィールドに結果が表示されます。

ステップ 10　Cisco IronPort スパム検疫でドメインベース クエリーを使用するには、[Designate as the active query] チェックボックスをオンにします。

（注）　ドメインベース クエリーが、指定されたクエリー タイプのアクティブ LDAP クエリーになります。たとえば、エンドユーザ認証にドメインベース クエリーを使用する場合、Cisco IronPort スパム検疫のアクティブなエンドユーザ認証クエリーになります。

ステップ 11　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

（注）　同じ設定をコマンド ライン インターフェイスで行うには、コマンド ライン プロンプトで、`ldapconfig` コマンドの `advanced` サブコマンドを入力します。

チェーン クエリー

チェーン クエリーは、AsyncOS によって順番に実行される一連の LDAP クエリーで構成されます。AsyncOS は、この「チェーン」に含まれる一連のクエリーを順に実行し、LDAP サーバから肯定的なレスポンスが返されるか、最後のクエリー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 クエリーが役立つのは、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、組織の各部門が、異なるタイプの LDAP ディレクトリを使用していることがあります。IT 部門が OpenLDAP を使用し、営業部門が Active Directory を使用しているとします。両方のタイプの LDAP ディレクトリに対して確実にクエリーを実行するには、チェーン クエリーを使用します。

チェーン クエリーを使用してエンドユーザ アクセスまたは Cisco IronPort スパム検疫の通知を制御するには、次の手順を実行します。

ステップ 1　チェーン クエリーで使用するクエリーごとに 1 つずつ、LDAP 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 プロファイルの作成」（P.10-3）を参照してください。

ステップ 2　チェーン クエリーを作成し、Cisco IronPort スパム検疫のアクティブ クエリーとして指定します。詳細については、「チェーン クエリーの作成」（P.10-15）を参照してください。

ステップ 3　Cisco IronPort スパム検疫に対して、LDAP エンドユーザ アクセスまたはスパム通知をイネーブルにします。スパム検疫の詳細については、「IronPort スパム検疫の設定」（P.7-3）を参照してください。

チェーン クエリーの作成

チェーン クエリーを作成するには、次の手順を実行します。

（または、CLI で `ldapconfig` コマンドの `advanced` サブコマンドを実行します）。

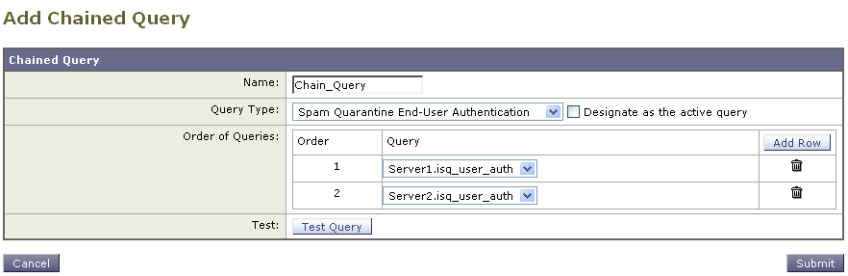
ステップ 1　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [LDAP] > [LDAP Server] を選択します。

ステップ 1　[LDAP Server Profiles] ページの [Advanced] をクリックします。

ステップ 2　[Add Chained Query] をクリックします。

[Add Chained Query] ページが表示されます。

図 10-3　　チェーン クエリーの設定



ステップ 3　チェーン クエリーの名前を入力します。

ステップ 4　クエリーのタイプを選択します。

チェーン クエリーを作成するときは、すべてのコンポーネント クエリーが同じクエリー タイプになります。クエリーのタイプを選択すると、該当するクエリーが LDAP からクエリー フィールド ドロップダウン リストに表示されます。

ステップ 5　チェーンの最初のクエリーを選択します。

Cisco IronPort アプライアンスによって、ここで設定した順にクエリーが実行されます。チェーン クエリーに複数のクエリーを追加した場合、一般的なクエリーが詳細なクエリーの後で実行されるように、並べ替えることがあります。

ステップ 6　[Test Query] ボタンをクリックし、[Test Parameters] フィールドにユーザのログインとパスワード、または電子メール アドレスを入力して、クエリーをテストします。[Connection Status] フィールドに結果が表示されます。

ステップ 7　Cisco IronPort スパム検疫でドメイン クエリーを使用するには、[Designate as the active query] チェックボックスをオンにします。

（注）　チェーン クエリーが、指定されたクエリー タイプのアクティブ LDAP クエリーになります。たとえば、エンドユーザ認証にチェーン クエリーを使用する場合、Cisco IronPort スパム検疫のアクティブなエンドユーザ認証クエリーになります。

ステップ 8　[Submit] をクリックし、[Commit] をクリックして変更を確定します。

（注）　同じ設定をコマンド ライン インターフェイスで行うには、コマンド ライン プロンプトで、ldapconfig コマンドの advanced サブコマンドを入力します。

AsyncOS を複数の LDAP サーバと連携させるための設定

LDAP サーバ プロファイルを設定するときに、Cisco IronPort 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、格納されている情報、構造、使用する認証情報を同一にする必要があります。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。

次の機能を使用する場合は、冗長 LDAP サーバに接続するように Cisco IronPort アプライアンスを設定します。

- **フェールオーバー**。Cisco IronPort アプライアンスが LDAP サーバに接続できない場合、リストで次に指定されているサーバに接続します。
- **ロード バランシング**。Cisco IronPort アプライアンスは、LDAP クエリーを実行するときに、リストで指定されている LDAP サーバの間で接続を分散します。

冗長 LDAP サーバを設定するには、[Management Appliance] > [System Administration] > [LDAP] ページまたは CLI の ldapconfig コマンドを使用します。

サーバとクエリーのテスト

[Add（または Edit）LDAP Server Profile] ページの [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 サーバでのクエリーのテストも実行されて、結果が個別に表示されます。

フェールオーバー

LDAP サーバで確実にクエリーを解決できるようにするには、フェールオーバー用に LDAP プロファイルを設定できます。

Cisco IronPort 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内の最初の LDAP サーバに接続できない場合は、リスト内の次の LDAP サーバへの接続が試行されます。Cisco IronPort アプライアンスが確実にプライマリ 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。

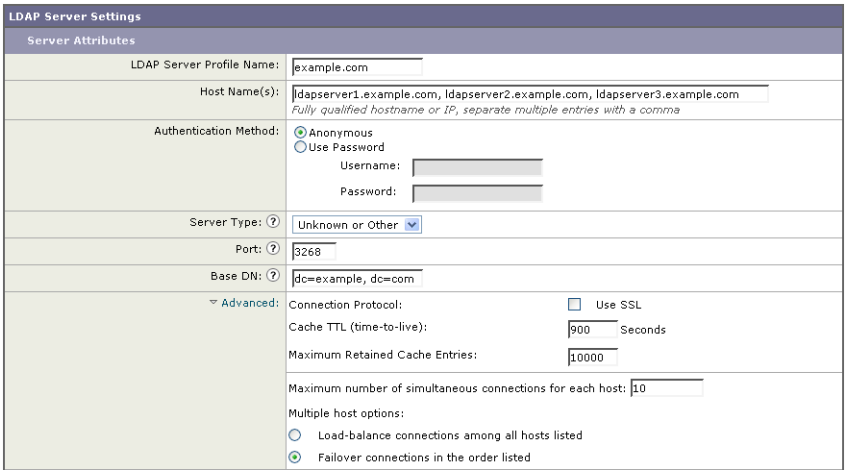
Cisco IronPort アプライアンスが 2 番目以降の LDAP サーバに接続した場合は、指定された時間が経過するまで、そのサーバに接続したままになります。この時間が経過すると、アプライアンスはリスト内の最初のサーバに対して再接続を試行します。

LDAP フェールオーバーのための Cisco IronPort 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 Cisco IronPort アプライアンスを設定するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [LDAP] を選択します。

[LDAP Server Setup] ページが表示されます。



ステップ 2　編集する LDAP サーバ プロファイルを選択します。

この例では、LDAP サーバ名が example.com です。

ステップ 3　[Hostname] テキスト フィールドに、LDAP サーバ（**ldapserver.example.com** など）を入力します。

ステップ 4　[Maximum number of simultaneous connections for each host] テキスト フィールドに、最大接続数を入力します。

この例では、最大接続数が **10** です。

ステップ 5　[Failover connections in the order list] の横にあるオプション ボタンをクリックします。

ステップ 6　その他の LDAP オプションを必要に応じて設定します。

ステップ 7　[Submit] をクリックし、[Commit] をクリックして保存します。

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 バランシングを使用した場合、Cisco IronPort 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、Cisco IronPort 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。Cisco IronPort 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。

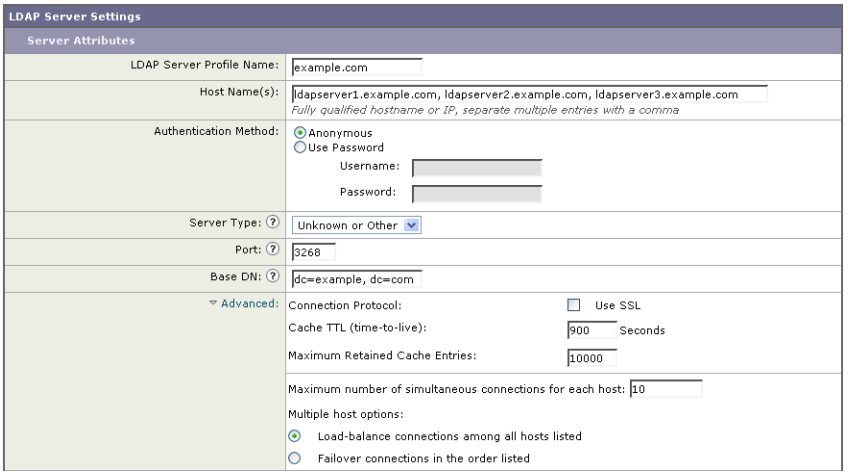
リストで指定された LDAP サーバの 1 つが応答しなくなった場合は、Cisco IronPort アプライアンスからの接続の負荷は残りの LDAP サーバに分散されます。

ロード バランシングのための Cisco IronPort アプライアンスの設定

LDAP ロード バランシングを行うように Cisco IronPort アプライアンスを設定するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [System Administration] > [LDAP] を選択します。

[LDAP Server Setup] ページが表示されます。



ステップ 2　編集する LDAP サーバ プロファイルを選択します。

この例では、LDAP サーバ名が example.com です。

ステップ 3　[Hostname] テキスト フィールドに、LDAP サーバ（**ldapserver.example.com** など）を入力します。

ステップ 4　[Maximum number of simultaneous connections for each host] テキスト フィールドに、最大接続数を入力します。

この例では、最大接続数が **10** です。

ステップ 5　[Load balance connections among all hosts] の横にあるオプション ボタンをクリックします。

ステップ 6　その他の LDAP オプションを必要に応じて設定します。

ステップ 7　[Submit] をクリックし、[Commit] をクリックして保存します。

ユーザの外部認証の設定

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 Cisco IronPort 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 ユーザ名とパスワード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ーを設定したら、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 [Management Appliance] > [System Administration] > [Users] ページまたは CLI の **userconfig** コマンドを使用します）。

ユーザの外部認証を設定するには、次の手順を実行します。

ステップ 1　**ユーザ アカウントを見つけ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ーを作成します。

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。**あるユーザがディレクトリ グループのメンバーであるかどうかを判断するクエリーを作成し、あるグループのすべてのメンバーを検索する別のクエリーを作成します。

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、『*Cisco IronPort AsyncOS for Email User Guide*』の「Adding Users」を参照してください。

（注）　[LDAP] ページの [Test Query] ボタン（または `ldaptest` コマンド）を使用して、クエリー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 クエリーのテスト」（P.10-11）を参照してください。

ユーザ アカウント クエリー

外部ユーザを認証するために、AsyncOS はクエリー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出し、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。管理者が選択したサーバ タイプに応じて、AsyncOS によってデフォルトのクエリーとデフォルトの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**）。ユーザのレコードがあるドメイン レベルのベース DN が必要です。

表 10-5 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ー文字列とユーザのフル ネーム属性を示します。

表 10-5　Active Directory サーバのデフォルト クエリー文字列

サーバ タイプ	Active Directory
ベース 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）
クエリー文字列	`(&(objectClass=user)(sAMAccountName={u}))`
ユーザのフル ネームが格納されている属性	`displayName`

表 10-6 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ー文字列とユーザのフル ネーム属性を示します。

表 10-6　Open LDAP サーバのデフォルト クエリー文字列

サーバ タイプ	OpenLDAP
ベース 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）
クエリー文字列	`(&(objectClass=posixAccount)(uid={u}))`
ユーザのフル ネームが格納されている属性	`gecos`

グループ メンバーシップ クエリー

AsyncOS も、ユーザがディレクトリ グループのメンバーであるかどうかを判断するクエリー、およびグループのすべてのメンバーを検索する別のクエリーを使用します。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 [Management Appliance] > [System Administration] > [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」というロールを割り当て、「Support」というディレクトリ グループのユーザに「Help Desk User」というロールを割り当てます。

ユーザが異なるユーザ ロールを持つ複数の LDAP グループに属する場合は、AsyncOS がユーザに最も制限されたロールの権限を割り当てます。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 クエリー文字列が 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ー文字列は (&(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。

表 10-7 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ー文字列と属性を示します。

表 10-7　Active Directory サーバのデフォルト クエリー文字列および属性

サーバ タイプ	Active Directory
ベース 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 member of 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。
グループのすべてのメンバーを判別するクエリー文字列	`(&(objectClass=group)(cn={g}))`
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`

表 10-8 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ー文字列と属性を示します。

表 10-8　Open LDAP サーバのデフォルト クエリー文字列および属性

サーバ タイプ	OpenLDAP
ベース 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}))`
グループのすべてのメンバーを判別するクエリー文字列	`(&(objectClass=posixGroup)(cn={g}))`
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`