LDAP との統合

この章は、次の項で構成されています。

概要

企業の LDAP ディレクトリ（例：Microsoft Active Directory、SunONE Directory Server、OpenLDAP ディレクトリなど）のエンド ユーザのパスフレーズおよび電子メール エイリアスを管理する場合、LDAP ディレクトリを使用して次のユーザを認証することができます。

- スパム隔離にアクセスするエンド ユーザおよび管理ユーザ。

  ユーザがスパム隔離の Web UI にログインする場合、LDAP サーバはログイン名とパスフレーズを検証し、AsyncOS は対応する電子メール エイリアスのリストを取得します。そのユーザの電子メール エイリアスのいずれかに送信された隔離メッセージは、アプライアンスが書き換えない限りスパム隔離で表示できます。

  スパム隔離と連携させるための LDAP の設定 （2 ページ） を参照してください。

- 外部認証が有効で、設定されている場合に、Cisco コンテンツ セキュリティ管理アプライアンスにサインインする管理ユーザ。

  LDAP を使用した管理ユーザの外部認証の設定 （16 ページ） を参照してください。

スパム隔離と連携させるための LDAP の設定

Cisco コンテンツ セキュリティ 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。

- サーバ名およびポート
- ベース DN（Base DN）
- サーバを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 （2 ページ） 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、AsyncOS からの接続先となる LDAP サーバを複数設定できます。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 （13 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 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隔離クエリを使用するか、または実際に使用する LDAP の実装とスキーマに合わせて自分のクエリを作成することができます。次に、スパム通知、および隔離へのエンドユーザ アクセス検証に使用するアクティブ クエリを指定します。

クエリの詳細については、LDAP クエリの設定 （5 ページ）を参照してください。

ステップ 3 スパム隔離に対して、LDAP エンドユーザ アクセスおよびスパム通知を有効にします。

スパム隔離への LDAP エンドユーザ アクセスを有効にして、エンドユーザが隔離内のメッセージを表示および管理できるようにします。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、中央集中型スパム隔離の設定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。

ステップ 1 （新しいWebインターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] を選択します。

ステップ 3 [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 4 [LDAPサーバプロファイル名（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 5 [ホスト名（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 （13 ページ）を参照してください。

ステップ 6 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。

（注） レポート上のクライアント 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。**[パスフレーズを使用（Use Passphrase）]** オプション ボタンを選択して、ユーザ名とパスフレーズを入力します。[ユーザメール概要（User Mail Summary）] ページにユーザ名が表示されます。

ステップ 7 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 8 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 Active Directory のデフォルト ポートであり、複数サーバ環境のグローバル カタログへのアクセスが可能になります。

ステップ 9 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、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、次のようになります。

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

- [オプション - LDAP グローバル設定で「LDAP サーバ証明書の検証」が有効な場合のみ（Optional - Only if "Validate LDAP Server Certificate" is enabled in LDAP Global Settings）]：サーバ証明書を検証するためにカスタム認証局をアップロードするかどうかを確認します。
- 認証局を追加するには、CLI で certconfig > CERTAUTHORITY サブコマンドを使用します。[オプション - LDAP グローバル設定で「LDAP サーバ証明書の検証」が有効で、FQDN 検証が SSL 設定で有効な場合のみ（Optional - Only if "Validate LDAP Server Certificate" is enabled in LDAP Global Settings and FQDN validation enabled in SSL Configuration settings）]：サーバ証明書にある [Common Name（共通

名）]、[SAN: DNS Name（SAN：DNS 名）] フィールド、またはその両方が FQDN 形式かどうかを確認します。

- [オプション - LDAP グローバル設定で「LDAP サーバ証明書の検証」が有効な場合のみ（Optional - Only if "Validate LDAP Server Certificate" is enabled in LDAP Global Settings）]：サーバ証明書の [Common Name（共通名）] または [SAN: DNS Name（SAN：DNS 名）] フィールドにサーバのホスト名が含まれているかどうかを確認します。[ホスト名（Hostname）] フィールドに IP が設定されている場合は、Reverse DNS 名が使用されます。

ステップ 10 [詳細設定（Advanced）] 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 11 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 12 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 13 同時接続の最大数を入力します。

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。詳細については、ロード バランシング （15 ページ）を参照してください。

（注） 同時接続の最大数には、LDAP クエリに使用される LDAP 接続が含まれます。ただし、スパム隔離の LDAP 認証を有効にした場合、アプライアンスはエンド ユーザ隔離に対して 20 の追加接続を許可し、接続の総数は 30 となります。

ステップ 14 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 （5 ページ）を参照してください。

ステップ 15 スパム隔離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。

ユーザがエンドユーザ隔離にログインするときにそのユーザを検証する、隔離エンドユーザ認証クエリを設定できます。エンドユーザが電子メール エイリアスごとに隔離通知を受け取らないように、エイリアス統合クエリを設定できます。これらの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ます。詳細については、LDAP クエリの設定 （5 ページ）を参照してください。

ステップ 16 [クエリのテスト（Test Query）] ボタンをクリックして、スパム隔離クエリをテストします。

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。

（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 17 変更を送信し、保存します。

Active Directory サーバ設定では、Windows 2000 で TLS 経由の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 および Windows 2003 の TLS 認証は、動作します。

（注） サーバ設定の数は無制限ですが、サーバごとに、エンドユーザ認証クエリを 1 つとエイリアス統合クエリを 1 つだけ設定できます。

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。

LDAP クエリの設定

次のセクションで、スパム隔離クエリのタイプごとに、デフォルトのクエリ文字列と設定の詳細を示します。

- **スパム隔離へのエンドユーザ認証のクエリ。**詳細については、スパム隔離へのエンドユーザ認証のクエリ （6 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 （8 ページ）を参照してください。

隔離でエンドユーザ アクセスまたはスパム通知の 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ます。隔離アクセスを制御するエンドユーザ認証クエリを 1 つと、スパム通知用のエイリアス統合クエリを 1 つ指定できます。既存のアクティブ クエリはすべてディセーブルになります。セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）]>[システム管理（System Administration）] > [LDAP] ページを選択します。アスタリスク（*）がアクティブ クエリの横に表示されます。

ドメインベースのクエリまたはチェーン クエリも、アクティブなエンドユーザ アクセス クエリまたはスパム通知クエリ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 （10 ページ）およびチェーン クエリ （12 ページ）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。

- LDAP クエリの構文 （6 ページ）
- 置換可能なトークン （6 ページ）

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。

置換可能なトークン

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
- {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、**(|(mail={a})(proxyAddresses=smtp:{a}))** になります。

（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 （9 ページ）を参照してください。

スパム隔離へのエンドユーザ認証のクエリ

エンドユーザ認証クエリとは、スパム隔離にログインする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。

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 **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}) というクエリ文字列を使用します。

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、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、メール属性は mail と proxyAddresses を使用しています。

表 *1 : 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 サーバの匿名認証、OpenLDAP サーバのエンドユーザ認証用のデフォルト クエリ文字列、mail および mailLocalAddress メール属性を使用します。

表 *2 : 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

認証方式	匿名（Anonymous）
[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	（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。

Active Directory サーバの場合、デフォルト クエリー文字列（実際の展開では異なることもあります）は (|(proxyAddresses={a})(proxyAddresses=smtp:{a})) で、デフォルトの電子メール属性は 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。

- Active Directory エイリアス統合の設定例 （8 ページ）
- OpenLDAP エイリアス統合の設定例 （9 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 *3 : 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

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 *4 : 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）
クエリ文字列	(mail={a}))
メール属性	メール アドレス

LDAP クエリのテスト

[LDAPサーバプロファイルの追加/編集（Add/Edit LDAP Server Profile）] ページの [クエリのテスト（Test Query）] ボタン（または CLI の ldaptest コマンド）を使用して、クエリをテストします。AsyncOS に、クエリ接続テストの各ステージの詳細が表示されます。たとえば、最初のステージの SMTP 認証に成功したか失敗したか、バインド照合の返された結果が true か false か、などです。

ldaptest コマンドを、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 と入力すると、maillocaladdress と入力する場合とは異なるクエリを実行します。

クエリをテストするには、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。[テスト接続（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が成功した場合、「成功：アクション：一致ポジティブ（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の場合は、統合されたスパム通知用の電子メール アドレスと共に、「成功：アクション：エイリアス統合（Success: Action: alias consolidation）」という結果が表示されます。クエリが失敗すると、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 コンテンツ セキュリティ アプライアンスは、LDAP サーバごとにクエリをテストします。

ドメインベース クエリ

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、ドメインに関連付けたものです。複数の別の LDAP サーバが異なるドメインに関連付けられているが、エンドユーザ隔離アクセスに対し、すべての LDAP サーバでクエリを実行する必要がある場合、ドメインベース クエリの使用を推奨します。たとえば、Bigfish という名前の会社が Bigfish.com、Redfish.com、および Bluefish.com というドメインを所持していて、それぞれのドメインに関連する従業員用に別の LDAP サーバを管理するとします。Bigfish は、ドメインベース クエリを使用して、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することができます。

ドメインベース クエリを使用してスパム隔離のエンドユーザ アクセスまたは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 クエリで使用する各ドメインについて LDAP サーバ プロファイルを作成します。各サーバ プロファイルでは、ドメインベース クエリで使用するクエリを設定します。詳細については、LDAP サーバ プロファイルの作成 （2 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に、各サーバ プロファイルからクエリを選択し、ドメインベース クエリをスパム隔離のアクティブ クエリとして指定します。クエリ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 （11 ページ）を参照してください。

ステップ 3 スパム隔離に対して、エンドユーザ アクセスおよびスパム通知を有効にします。詳細については、Web ブラウザからのスパム隔離へのエンドユーザ アクセスの設定を参照してください。

ドメインベース クエリの作成

ステップ 1 （新しいWebインターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] を選択します。

ステップ 3 [LDAP] ページで、[詳細設定（Advanced）] をクリックします。

ステップ 4 ドメインベース クエリーの名前を入力します。

ステップ 5 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は、シングル クエリ タイプを指定します。クエリのタイプを選択すると、該当するクエリが LDAP サーバ プロファイルからクエリ フィールド ドロップダウン リストに含まれるようになります。

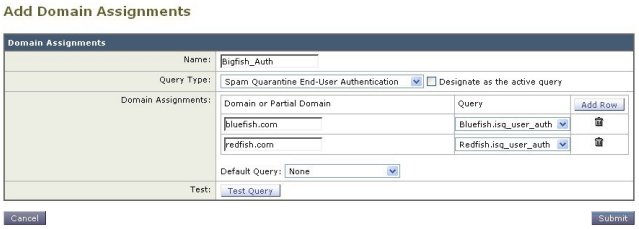
ステップ 6 [ドメイン割り当て（Domain Assignments）] フィールドに、ドメインを入力します。

ステップ 7 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 8 行を追加して、ドメインベース クエリのドメインごとにクエリを選択します。

ステップ 9 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します。デフォルトのクエリを入力しない場合は、[なし（None）] を選択します。

図 *1*: ドメインベース クエリの例



ステップ 10 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 11 スパム隔離でドメインベース 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ます。

（注） ドメインベース クエリが、指定されたクエリ タイプのアクティブ LDAP クエリになります。たとえば、ドメインベース クエリがエンドユーザ認証に使用されている場合は、スパム隔離のアクティブ エンドユーザ認証クエリになります。

ステップ 12 [送信（Submit）] をクリックし、[確定する（Commit）] をクリックして変更を保存します。

（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

チェーン クエリは、AsyncOS が連続して実行する一連の LDAP クエリです。AsyncOS は LDAP サーバから肯定的なレスポンスが返されるまで、または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まで、シリーズ内の各クエリ、「チェーン」内の各クエリを実行します。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、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。クエリが両方のタイプの LDAP ディレクトリに対して実行されていることを確認するために、チェーン クエリを使用できます。

チェーン クエリを使用してスパム隔離のエンドユーザ アクセスまたは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 クエリで使用するクエリごとに 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 （2 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、スパム隔離のアクティブ クエリとして指定します。詳細については、チェーン クエリの作成 （12 ページ）を参照してください。

ステップ 3 スパム隔離に対して、LDAP エンドユーザ アクセスおよびスパム通知を有効にします。スパム隔離の詳細については、「中央集中型スパム隔離の設定」を参照してください。

チェーン クエリの作成

ヒント CLI から、ldapconfig コマンドの advanced サブコマンドも使用できます。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] > [LDAPサーバ（LDAP Server）] を選択します。

ステップ 3 [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 4 [連鎖クエリを追加（Add Chained Query）] をクリックします。

ステップ 5 チェーン クエリの名前を入力します。

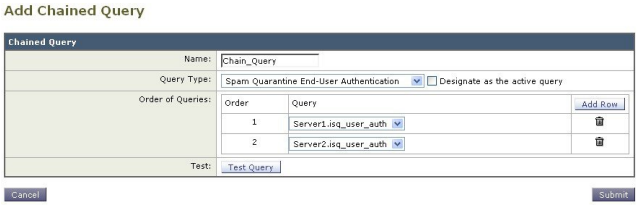
ステップ 6 クエリのタイプを選択します。

チェーン クエリを作成するときは、そのコンポーネントのクエリすべてを同じクエリ タイプにします。クエリのタイプを選択すると、該当するクエリが LDAP からクエリ 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 7 チェーンの最初のクエリを選択します。

Cisco コンテンツ セキュリティ 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。チェーン クエリに複数のクエリを追加する場合は、詳細なクエリの後に広範なクエリが続くように順序付けることを推奨します。

図 *2:* チェーン クエリの例



ステップ 8 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、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 9 スパム隔離でドメイン 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ます。

（注） チェーン クエリが、指定されたクエリ タイプのアクティブ LDAP クエリになります。たとえば、チェーン クエリがエンドユーザ認証に使用されている場合は、スパム隔離のアクティブ エンドユーザ認証クエリになります。

ステップ 10 変更を送信し、保存します。

（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 コンテンツ セキュリティ 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 コンテンツ セキュリティ アプライアンスを設定します。

- **フェールオーバー**。Cisco コンテンツ セキュリティ 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 コンテンツ セキュリティ アプライアンスは、LDAP クエリを実行するときに、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、[管理アプライアンス（Management Appliance）] > [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。

サーバとクエリのテスト

[LDAP サーバ プロファイルを追加（または編集）（Add (or 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。

フェールオーバー

LDAP サーバで確実にクエリ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。LDAP サーバへの接続が失敗するか、またはクエリからエラーが返される場合にそうすることが適切であれば、アプライアンスはリストに指定されている次の LDAP サーバに対してクエリを試行します。

Cisco コンテンツ セキュリティ 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、またはクエリからエラーが返される場合、リスト内の次の LDAP サーバへの接続が試行されます。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。Cisco コンテンツ セキュリティ 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。

（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。

Cisco コンテンツ セキュリティ アプライアンスが 2 番目の、または後続の LDAP サーバに接続する場合、そのサーバへの接続は所定の時間が経過するまで維持されます。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 コンテンツ セキュリティ アプライアンスの設定

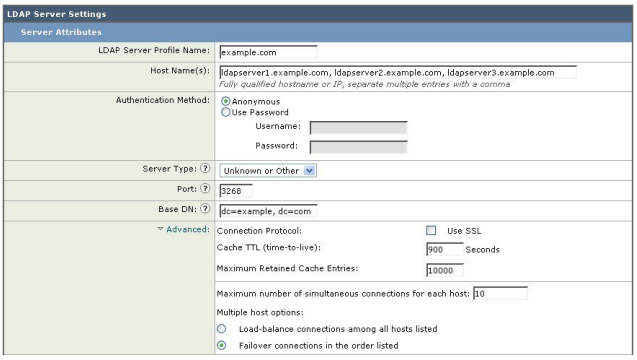
ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] を選択します。

ステップ 3 編集する LDAP サーバ プロファイルを選択します。

次の例で、LDAP サーバ名は example.com です。

図 *3 : LDAP* フェールオーバー コンフィギュレーションの例



ステップ 4 [ホスト名（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 5 [各ホストの最大同時接続数（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 6 [一覧されている順序での接続のフェールオーバー（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 7 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 8 変更を送信し、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 コンテンツ セキュリティ 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。

ロード バランシングのための Cisco コンテンツ セキュリティ アプライアンスの設定

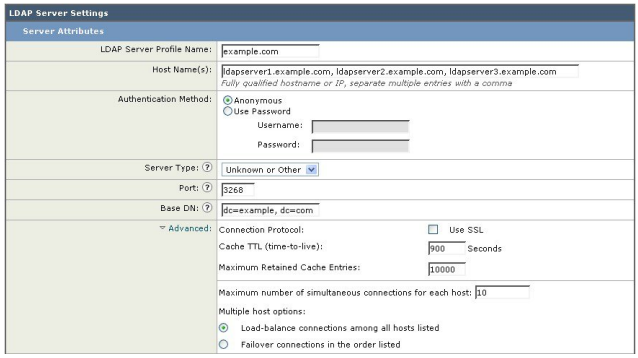
ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] を選択します。

ステップ 3 編集する LDAP サーバ プロファイルを選択します。

次の例で、LDAP サーバ名は example.com です。

図 *4:* ロードバランシングの設定例



ステップ 4 [ホスト名（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 5 [各ホストの最大同時接続数（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 6 [すべてのホスト間での負荷分散接続（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 7 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 8 変更を送信し、保存します。

LDAP を使用した管理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管理ユーザを認証するように Cisco コンテンツ セキュリティ 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、アプライアンスにログインできるようになります。

ステップ 1 **LDAP サーバ プロファイルを設定します。**LDAP サーバ プロファイルの作成 （2 ページ）を参照してください。

ステップ 2 **ユーザ アカウントを見つけるためのクエリを作成します。**LDAP サーバ プロファイルの、[外部認証クエリ（External Authentication Queries）] セクションで、クエリを作成して LDAP ディレクトリ内のユーザ アカウントを検索します。管理ユーザの認証のためのユーザ アカウント クエリ （17 ページ）を参照してください。

ステップ 3 **グループ メンバーシップ クエリを作成します。**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を作成します。詳細については、管理ユーザの認証のためのグループ メンバーシップ クエリ （18 ページ）およびご使用の E メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプを参照してください。

（注） そのページの [外部認証クエリ（External Authentication Queries）] セクションにある [テスト クエリ（Test Queries）] 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。関連情報については、LDAP クエリのテスト （9 ページ） を参照してください。

ステップ 4 **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、管理ユーザの外部認証のイネーブル化 （20 ページ）および E メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Adding Users」を参照してください。

管理ユーザの認証のためのユーザ 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 *5 : Active Directory* サーバのデフォルト クエリ文字列

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}))

サーバ タイプ（Server Type）	Active Directory
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 *6 : Open LDAP* サーバのデフォルト クエリ文字列

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

管理ユーザの認証のためのグループ メンバーシップ クエリ

LDAP グループをアプライアンスにアクセスするためのユーザ ロールと関連付けることができます。

AsyncOS は、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や、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を使用することもできます。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 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] ページ（または CLI の userconfig）で外部認証を有効にするときに、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、グループ メンバーのユーザ名が格納されている属性、および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 *7 : Active Directory* サーバのデフォルト クエリ文字列および属性

クエリ文字列	**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 スキーマにおいてメンバーの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

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 *8 : Open LDAP* サーバのデフォルト クエリ文字列および属性

クエリ文字列	**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}))
グループのすべてのメンバーを判別するクエリ文字列	(&(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

管理ユーザの外部認証のイネーブル化

LDAP サーバプロファイルおよびクエリを設定した後で、LDAP を使用する外部認証をイネーブルにすることができます。

ステップ 1 （新しいWebインターフェイスのみ）セキュリティ管理アプライアンスで をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] ページを選択します。

ステップ 3 [有効（Enable）] をクリックします。

ステップ 4 [外部認証を有効にする（Enable External Authentication）] チェックボックスをオンにします。

ステップ 5 認証タイプとして [LDAP] を選択します。

ステップ 6 ユーザを認証する LDAP 外部認証クエリーを選択します。

ステップ 7 タイムアウトするまでアプライアンスがサーバからの応答を待つ時間を秒単位で入力します。

ステップ 8 アプライアンスで認証する LDAP ディレクトリからのグループ名を入力し、グループのユーザに対するロールを選択します。

ステップ 9 また、[行の追加（Add Row）] をクリックして別のディレクトリ グループを追加することもできます。アプライアンスが認証する各ディレクトリ グループに対してステップ 7 とステップ 8 を繰り返します。

ステップ 10 変更を送信し、保存します。