# セキュア LDAP（SLDAP）


- SLDAP について （1 ページ）
- SLDAP の設定の前提条件 （3 ページ）
- SLDAP の設定の制約事項 （3 ページ）
- SLDAP の設定 （3 ページ）
- AAA サーバ グループの設定（GUI） （4 ページ）
- AAA サーバ グループの設定 （6 ページ）
- 認証要求のための検索操作とバインド操作の設定 （7 ページ）
- SLDAP サーバでのダイナミック属性マップの設定 （7 ページ）
- SLDAP の設定の確認 （8 ページ）


## SLDAP について

### Transport Layer Security（TLS）

Transport Layer Security（TLS）は、プライバシー、認証、およびデータ整合性によるデータのセキュア トランザクションを可能にするアプリケーションレベル プロトコルです。TLS は、証明書、公開キーおよび秘密キーに基づいて、クライアントの ID を証明します。

証明書は認証局（CA）によって発行されます。

各証明書には次のものが含まれています。

- 発行された権限の名前。
- 証明書の発行先エンティティの名前。
- エンティティの公開キー。
- 証明書の有効期限を示すエンティティのタイムスタンプ。

TLS による LDAP のサポートについては、LDAP プロトコルの拡張である RFC 2830 を参照してください。

### LDAP 操作

バインド

バインド操作は、サーバに対してユーザを認証するために使用されます。LDAP サーバとの接続を開始するために使用されます。LDAP はコネクション型プロトコルです。クライアントはプロトコル バージョンと認証情報を指定します。

LDAP は次のバインドをサポートします。

- 認証済みバインド：認証済みバインドは、ルートの認定者名（DN）とパスワードが使用できる場合に実行されます。
- 匿名バインド：ルート DN とパスワードがない場合は、匿名バインドが実行されます。

LDAP 環境では、検索操作が実行されてから、バインド操作が実行されます。これは、パスワード属性が検索操作の一部として返される場合、パスワードの確認を LDAP クライアントのローカルで実行できるためです。したがって、余計なバインド操作を実行する必要がなくなります。パスワード属性が返されない場合、バインド操作を後で実行できます。検索操作を先に実行してバインド操作を後で実行するもう 1 つの利点は、ユーザ名（cn 属性）の前にベース DN を付けることで DN を構成するのではなく、検索結果で受信した DN をユーザ DN として使用できることです。LDAP サーバに保存されているすべてのエントリには、固有の DN があります。

DN は 2 つの部分で構成されます。

- 相対識別名（RDN）
- レコードが存在する LDAP サーバ内の場所。

LDAP サーバに保存されているエントリのほとんどには名前があり、多くの場合、名前は Common Name（cn）属性で保存されます。すべてのオブジェクトには名前があるため、LDAP に保存されているほとんどのオブジェクトは RDN のベースとして cn 値を使用します。

検索

検索操作は、LDAP サーバを検索するために使用されます。クライアントは検索の開始点（ベース DN）、検索範囲（オブジェクト、その子、またはそのオブジェクトをルートとするサブツリー）、およびサーチ フィルタを指定します。

認可要求の場合、検索操作はバインド操作なしで直接実行されます。検索操作を正常に実行するには、LDAP サーバを特定の特権で設定します。この特権レベルは、バインド操作で設定します。

LDAP 検索操作は、特定のユーザについて複数のユーザ エントリを返す可能性があります。このような場合、LDAP クライアントは適切なエラー コードを AAA に返します。このようなエラーを回避するために、単一のエントリに一致させるための適切なサーチ フィルタを設定する必要があります。

比較

認証のために、比較操作を使用して、バインド要求を比較要求で置換します。比較操作によって、接続のための最初のバインド パラメータを維持できます。

### LDAP ダイナミック属性マッピング

Lightweight Directory Access Protocol（LDAP）は、AAA サーバとの通信に適した強力で柔軟性の高いプロトコルです。LDAP 属性マップには、サーバから取得した属性を、セキュリティアプライアンスによってサポートされるシスコ属性にクロスリファレンスする方式が備わっています。

ユーザがセキュリティアプライアンスを認証すると、次にセキュリティアプライアンスはサーバを認証し、LDAP プロトコルを使用してそのユーザのレコードを取得します。このレコードは、サーバにユーザ インターフェイスに表示されるフィールドに関連付けられた LDAP 属性で構成されます。取得される各属性には、ユーザ レコードを更新する管理者が入力した値が含まれます。

# SLDAP の設定の前提条件

セキュア Transport Layer Security（TLS）のセキュア接続を使用している場合、 X.509 証明書を設定する必要があります。

# SLDAP の設定の制約事項

- LDAP 照会はサポートされていません
- LDAP サーバからの割り込みメッセージまたは通知は処理されません。
- LDAP 認証は、インタラクティブ（端末）セッションではサポートされていません。

# SLDAP の設定

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Device# enable` | 特権 EXEC モードをイネーブルにします。<br>パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>`Device# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ldap server** *name*<br>例： | Lightweight Directory Access Protocol（LDAP）サーバを定義し、LDAP サー |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device(config)# ldap server server1` | バ コンフィギュレーション モードを開始します。 |
| ステップ 4 | **ipv4** *ipv4-address*<br>例：<br>`Device(config-ldap-server)# ipv4 9.4.109.20` | IPv4 を使用して LDAP サーバの IP アドレスを指定します。 |
| ステップ 5 | **timeout retransmit** *seconds*<br>例：<br>`Device(config-ldap-server)# timeout retransmit 20` | Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ 組み込みワイヤレスコントローラが LDAP 要求を再送信する前に応答を待機する秒数を指定します。 |
| ステップ 6 | **bind authenticate root-dn password** [**0** *string* \| **7** *string*] *string*<br>例：<br>`Device(config-ldap-server)# bind authenticate root-dn CN=ldapipv6user,CN=Users,DC=ca,DC=ssh2,DC=com password Cisco12345` | Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ 組み込みワイヤレスコントローラと LDAP サーバ間で使用される共有秘密テキスト ストリングを指定します。<br>暗号化されていない共有秘密を設定するには、**0** 回線オプションを使用します。<br>暗号化された共有秘密を設定するには、**7** 回線オプションを使用します。 |
| ステップ 7 | **base-dn** *string*<br>例：<br>`Device(config-ldap-server)# base-dn CN=Users,DC=ca,DC=ssh2,DC=com` | 検索のベース識別名（DN）を指定します。 |
| ステップ 8 | **mode secure** [**no- negotiation**]<br>例：<br>`Device(config-ldap-server)# mode secure no- negotiation` | TLS 接続を開始するよう LDAP を設定し、セキュア モードを指定します。 |
| ステップ 9 | **end**<br>例：<br>`Device(config-ldap-server)# end` | 特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。 |

# AAA サーバ グループの設定（GUI）

AAA サーバ グループを使用するようにデバイスを設定すると、既存のサーバ ホストをグループ化し、設定済みのサーバ ホストのサブセットを選択して、それらのサーバを特定のサービスに使用することが簡単にできます。サーバ グループは、グローバル サーバ ホストの一覧と一

緒に使用されます。サーバ グループには、選択したサーバ ホストの IP アドレスが一覧表示されます。

次のサーバ グループを作成できます。

### 手順

**ステップ 1** RADIUS

a) [Services] > [Security] > [AAA] > [Server Groups] > [RADIUS] を選択します。
b) [Add] ボタンをクリックします。[Create AAA Radius Server Group] ダイアログボックスが表示されます。
c) [Name] フィールドに、RADIUS サーバ グループの名前を入力します。
d) [MAC-Delimiter] ドロップダウン リストから目的の区切り文字を選択します。コロン、ハイフン、およびシングルハイフンから選択できます。
e) [MAC-Filtering] ドロップダウン リストから目的のフィルタを選択します。[mac] および [Key] を選択できます。
f) サーバを非稼働にするには、[Dead-Time (mins)] フィールドに値を入力します。値は 1 ～ 1440 の範囲で指定する必要があります。
g) [Available Servers] リストから使用可能なサーバを選択し、[>] ボタンをクリックして [Assigned Servers] リストに移動します。
h) [Save & Apply to Device] ボタンをクリックします。

**ステップ 2** TACACS+

a) [Services] > [Security] > [AAA] > [Server Groups] > [TACACS+] を選択します。
b) [Add] ボタンをクリックします。[Create AAA Tacacs Server Group] ダイアログボックスが表示されます。
c) [Name] フィールドに、TACACS サーバ グループの名前を入力します。
d) [Available Servers] リストから使用可能なサーバを選択し、[>] ボタンをクリックして [Assigned Servers] リストに移動します。
e) [Save & Apply to Device] ボタンをクリックします。

**ステップ 3** LDAP

a) [Services] > [Security] > [AAA] > [Server Groups] > [LDAP] を選択します。
b) [Add] ボタンをクリックします。[Create AAA Ldap Server Group] ダイアログボックスが表示されます。
c) [Name] フィールドに、LDAP サーバ グループの名前を入力します。
d) [Available Servers] リストから使用可能なサーバを選択し、[>] ボタンをクリックして [Assigned Servers] リストに移動します。
e) [Save & Apply to Device] ボタンをクリックします。

# AAA サーバ グループの設定

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Device# enable` | 特権 EXEC モードをイネーブルにします。<br>パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>`Device# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **aaa new-model**<br>例：<br>`Device(config)# aaa new-model` | AAA をイネーブルにします。 |
| ステップ 4 | **aaa group server ldap** *group-name*<br>例：<br>`Device(config)# aaa group server ldap name1` | グループ名を使用して AAA サーバ グループを定義し、LDAP サーバ グループ コンフィギュレーション モードを開始します。<br>グループのすべてのメンバは、タイプを同じにする必要があります。つまり、RADIUS、LDAP、または TACACS+ です。 |
| ステップ 5 | **server** *name*<br>例：<br>`Device(config-ldap-sg)# server server1` | 特定の LDAP サーバを定義済みのサーバ グループと関連付けます。<br>セキュリティ サーバは、IP アドレスと UDP ポート番号で識別されます。 |
| ステップ 6 | **exit**<br>例：<br>`Device(config-ldap-sg)# exit` | LDAP サーバ グループ コンフィギュレーション モードを終了します。 |

# 認証要求のための検索操作とバインド操作の設定

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Device# enable` | 特権 EXEC モードをイネーブルにします。<br>パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>`Device# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **aaa new-model**<br>例：<br>`Device(config)# aaa new-model` | AAA をイネーブルにします。 |
| ステップ 4 | **ldap server** *name*<br>例：<br>`Device(config)# ldap server server1` | Lightweight Directory Access Protocol（LDAP）サーバを定義し、LDAP サーバ コンフィギュレーション モードを開始します。 |
| ステップ 5 | **authentication bind-first**<br>例：<br>`Device(config-ldap-server)# authentication bind-first` | 認証要求のために一連の検索操作とバインド操作を設定します。 |
| ステップ 6 | **authentication compare**<br>例：<br>`Device(config-ldap-server)# authentication compare` | バインド要求を認証の比較要求に置き換えます。 |
| ステップ 7 | **exit**<br>例：<br>`Device(config-ldap-server)# exit` | LDAP サーバ グループ コンフィギュレーション モードを終了します。 |

# SLDAP サーバでのダイナミック属性マップの設定

既存のユーザ定義属性名と値を、セキュリティアプライアンスと互換性があるシスコ属性名と値にマッピングする、LDAP 属性マップを作成する必要があります。作成した属性マップは、必要に応じて LDAP サーバにバインドしたり削除したりできます。

（注） 属性マッピング機能を適切に使用するには、シスコ LDAP 属性の名前と値、およびユーザ定義属性の名前と値を理解する必要があります。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Device# enable` | 特権 EXEC モードをイネーブルにします。<br>パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>`Device# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ldap attribute-map** *map-name*<br>例：<br>`Device(config)# ldap attribute-map map1` | ダイナミック LDAP 属性マップを設定し、属性マップ コンフィギュレーション モードを開始します。 |
| ステップ 4 | **map type** *ldap-attr-type aaa-attr-type*<br>例：<br>`Device(config-attr-map)# map type department supplicant-group` | 属性マップを定義します。 |
| ステップ 5 | **exit**<br>例：<br>`Device(config-attr-map)# exit` | 属性マップ コンフィギュレーション モードを終了します。 |

# SLDAP の設定の確認

デフォルトの LDAP 属性マッピングの詳細を表示するには、次のコマンドを使用します。

```
Device# show ldap attributes
```

LDAP サーバの状態情報や、それ以外のサーバの各種カウンタを表示するには、次のコマンドを使用します。

```
Device# show ldap server
```