LDAP サーバと統合するための ISE の設定

目次

概要

このドキュメントでは、Cisco Identity Services Engine（ISE）を設定して Cisco Lightweight Directory Access Protocol（LDAP）サーバと統合する方法について説明します。

> **注:** このドキュメントは、LDAP を ISE 認証および承認のための外部 ID ソースとして使用するセットアップに適用されます。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- パッチ 2 が適用された Cisco ISE バージョン 1.3

- OpenLDAP がインストールされた Microsoft Windows 7 x64
- Cisco Wireless LAN Controller（WLC）バージョン 8.0.100.0
- Microsoft Windows 向け Cisco AnyConnect バージョン 3.1
- Cisco Network Access Manager プロファイル エディタ

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

LDAP では、次の認証方式がサポートされます。

- Extensible Authentication Protocol - Generic Token Card（EAP-GTC）
- Extensible Authentication Protocol - Transport Layer Security（EAP-TLS）
- Protected Extensible Authentication Protocol - Transport Layer Security（PEAP-TLS）

設定

ここでは、ネットワーク デバイスを設定して ISE に LDAP サーバを統合する方法を説明します。

ネットワーク図

この設定例では、エンドポイントでワイヤレス アダプタを使用してワイヤレス ネットワークに関連付けます。 WLC 上のワイヤレス LAN（WLAN）は、ISE を介してユーザを認証するように設定します。 ISE では、LDAP を外部 ID ストアとして設定します。

次の図に、この設定例で使用するネットワーク トポロジを示します。

OpenLDAP の設定

OpenLDAP for Microsoft Windows は、GUI を使用して簡単にインストールできます。 デフォルトの場所は **C: > OpenLDAP** です。 インストールが完了すると、このデレクトリは次のように表示されます。

次の 2 つのディレクトリに注目してください。

- **ClientTools**：このディレクトリには、LDAP データベースを編集するために使用する一連のバイナリが格納されています。

• **ldifdata**：LDAP オブジェクトを設定したファイルは、ここに保管する必要があります。

次に示す構造を LDAP データベースに追加してください。

ルート ディレクトリの下に、2 つの組織単位（OU）を設定する必要があります。 *OU=groups* OU には 1 つの子グループを持たせます（この例では **cn=domainusers**）。 *OU=people* OU は、*cn=domainusers* グループに属する 2 つのユーザ アカウントを定義します。

データベースにデータを取り込むには、最初に *ldif* ファイルを作成する必要があります。 前述の構造は、次のファイルを基に作成されたものです。

```
dn: ou=groups,dc=maxcrc,dc=com
changetype: add
ou: groups
description: All groups in organisation
objectclass: organizationalunit

dn: ou=people,dc=maxcrc,dc=com
changetype: add
ou: people
description: All people in organisation
objectclass: organizationalunit

dn: uid=john.doe,ou=people,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: john.doe
givenName: John
sn: Doe
cn: John Doe
mail: john.doe@example.com
userPassword: password

dn: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: jan.kowalski
givenName: Jan
sn: Kowalski
cn: Jan Kowalski
mail: jan.kowalski@example.com
userPassword: password

dn: cn=domainusers,ou=groups,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: posixGroup
gidNumber: 678
memberUid: uid=john.doe,ou=people,dc=maxcrc,dc=com
memberUid: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com
```

LDAP データベースにオブジェクトを追加するには、**ldapmodify** バイナリを使用できます。

```
C:\OpenLDAP\ClientTools>ldapmodify.exe -a -x -h localhost -p 389 -D "cn=Manager,
```

```
dc=maxcrc,dc=com" -w secret -f C:\OpenLDAP\ldifdata\test.ldif
ldap_connect_to_host: TCP localhost:389
ldap_new_socket: 496
ldap_prepare_socket: 496
ldap_connect_to_host: Trying ::1 389
ldap_pvt_connect: fd: 496 tm: -1 async: 0
attempting to connect:
connect success
adding new entry "ou=groups,dc=maxcrc,dc=com"

adding new entry "ou=people,dc=maxcrc,dc=com"

adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com"

adding new entry "uid=jan.kowalski,ou=people,dc=maxcrc,dc=com"

adding new entry "cn=domainusers,ou=groups,dc=maxcrc,dc=com"
```

OpenLDAP と ISE の統合

ISE に LDAP を外部 ID ストアとして設定するには、この項全体を通して記載する図を参考にしてください。

[General] タブで次の属性を設定します。:

- **Subject Objectclass**：このフィールドは、*ldif* ファイル内に設定されたユーザ アカウントのオブジェクト クラスに対応します。 LDAP 設定に応じて、次の 4 つのクラスのいずれかを使用できます。

  Top

  Person

  OrganizationalPerson

  InetOrgPerson

- **Subject Name Attribute**：ISE が特定のユーザ名がデータベースに保管されているかどうかを問い合わせると、LDAP はこの属性から値を取得します。 このシナリオでは、エンドポイントのユーザ名として **john.doe** または **jan.kowalski** を使用します。

- **Group Objectclass**：このフィールドは、*ldif* ファイル内に設定されたグループのオブジェクト クラスに対応します。 このシナリオでは、*cn=domainusers* グループのオブジェクト クラスは **posixGroup** です。

- **Group Map Attribute**：この属性は、どのようにユーザがグループにマッピングされるかを定義します。 *ldif* ファイル内の *cn=domainusers* グループの下に、ユーザに対応する 2 つの *memberUid* 属性があります。

ISE には、事前設定されたスキーマ（Microsoft Active Directory、Sun、Novell）も用意されています。

正しい IP アドレスと管理ドメイン設定した後、サーバとのバインディングのテスト を実行できます。 この時点では検索ベースがまだ設定されていないので、サブジェクトやグループを取得しないでください、

次のタブで、サブジェクト/グループの検索ベースを設定できます。 これが、ISE と LDAP の*結合*ポイントになります。 取得できるサブジェクトとグループは、統合ポイントの子となっているものだけです。 このシナリオでは、サブジェクトは *OU=people* からを取得され、グループは *OU=groups* から取得されます。

[Groups] タブで、LDAP から ISE にグループをインポートできます。、

WLC の設定

以下の図を参考に、802.1x 認証に対応するよう WLC を設定してください。

EAP-GTC の設定

EAP-GTC は、LDAP でサポートされる認証方式の 1 つです。 Cisco AnyConnect ではこの認証方式を使用できますが、それには Network Access Manager プロファイル エディタをインストールして、プロファイルを正しく設定する必要があります。 また、Network Access Manager の設定を編集する必要もあります。この設定は、デフォルトでは次の場所にあります。

C： \ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml file

以下の図を参考に、エンドポイントに EAP-GTC を設定してください。

以下の図を参考に、ISE の認証および承認ポリシーを変更してください。

以上の設定を適用すると、ネットワークに接続できるようになっているはずです。

確認

LDAP および ISE の設定を検証するには、サーバとのテスト接続で、サブジェクトと h グループを取得できる状態でなければなりません。

以下の図に、ISE からのレポート例を示します。

トラブルシューティング

ここでは、この設定で発生する一般的なエラーと、そのトラブルシューティング方法を説明します。

- OpenLDAP をインストールした後、**gssapi.dll** が見つからないことを意味するエラーが発生する場合があります。 エラーを解消するには、Microsoft Windows を再起動する必要があります。

- Cisco AnyConnect の *configuration.xml* ファイルを直接編集できない場合があります。 新しい構成を別の場所に保存してから、そのファイルで古いファイルを置き換えてください。

- 認証レポートに、次のエラーが示される場合があります。

  `Authentication method is not supported by any applicable identity store`
  このエラー メッセージは、選択した認証方式が LDAP でサポートされないことを意味します。 同じレポート内に、*認証プロトコル* としてサポートされている方式（EAP-GTC、EAP-TLS、PEAP-TLS）のいずれかが示されていることを確認してください。

- 認証レポートに、サブジェクトが ID ストアで見つからなかったことが示される場合があります。 これは、レポートに示されているユーザ名と一致する [Subject Name] 属性を持つユーザが LDAP データベース内で見つからなかったことを意味します。 このシナリオでは、この属性の値が **uid** に設定されているため、ISE は一致を見つけようとするときに、LDAP ユーザの *uid* 値を調べます。

- *サーバとのバインディング* テスト中に、サブジェクトとグループが取得されない場合があります。 この問題の原因として最も可能性が高いのは、検索ベースが誤って設定されていることです。 LDAP 階層は、リーフからルートの方向および *dc*（複数の単語で構成可能）で指定する必要があることに注意してください。

  ヒント： WLC 側で EAP 認証をトラブルシューティングする方法については、シスコのドキュメント「WLAN コントローラ（WLC）での EAP 認証の設定例」を参照してください。