Cisco IOS ヘッドエンド上で LDAP を使用する AnyConnect クライアントに対するポリシー グループ割り当ての設定例

目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[設定](#)
[ネットワーク図](#)
[警告](#)
[確認](#)
[トラブルシューティング](#)

概要

この資料に自動的に資格情報に基づいてユーザに正しい VPN ポリシーを割り当てるために Lightweight Directory Access Protocol （ LDAP ） アトリビュート マップを設定する方法を記述されています。

> **注:** Cisco IOS ® ヘッドエンドに接続する Secure Sockets Layer VPN （ SSL VPN ）ユーザ向けの LDAP認証のためのサポートは Cisco バグ ID CSCuj20940 によってトラッキングされます。 サポートが公式に追加されるまで、LDAP サポートは最もよい努力です。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- SSL VPN on Cisco IOS
- Cisco IOS での LDAP 認証
- ディレクトリ サービス

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。

- CISCO881-SEC-K9
- Cisco IOS Software, C880 Software (C880DATA-UNIVERSALK9-M), Version 15.1(4)M, RELEASE SOFTWARE (fc1)

このドキュメントの情報は、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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

LDAP は Internet Protocol （ IP ） ネットワーク上の分散 ディレクトリ 情報サービスにアクセスし、維持する開いた、ベンダを問わない、業界標準アプリケ– ションプロトコルです。 ディレクトリ サービスはネットワーク全体のユーザ、システム、ネットワーク、サービスおよびアプリケーションについての情報の共有を許可すると同時にイントラネットおよびインターネットアプリケーションの開発の重要なロールを担います。

通常、管理者は、VPN ユーザにさまざまなアクセス権限または WebVPN コンテンツを提供します。 これは資格情報に各ユーザ依存へのこれらのポリシー セットの VPN サーバおよび割り当ての異なる VPN ポリシーの設定と完了することができます。 これは手動で完了することができる間、ディレクトリ サービスを用いるプロセスを自動化する効率的です。 ユーザにグループ ポリシーを割り当てるのに LDAP を使用するためにアトリビュートに VPN ヘッドエンドによって理解される Active Directory （ AD ） アトリビュート「memberOf」のような LDAP アトリビュートをマッピング する マップを設定する必要があります。

で適応型セキュリティ アプライアンス（ ASA ）ソフトウェア（ ASA ）これは LDAP アトリビュート マップ設定例の ASA 使用に示すように LDAP アトリビュート マップの異なるユーザーへの異なるグループ ポリシーの割り当てによって規則的に実現します。

Cisco IOS で同じ事柄を WebVPN コンテキストの下の異なるポリシー グループの設定と達成することができ、どのポリシー グループをユーザが割り当てられるか判別するために LDAP アトリビュートの使用はマッピング します。 on Cisco IOS ヘッドエンドは認証、許可、アカウンティング（ AAA ） アトリビュート サプリカント グループに、「memberOf」AD アトリビュート マッピング されます。 詳細については既定の属性マッピングで、ダイナミック アトリビュート マップ設定例を使用して IOSデバイスの LDAP を参照して下さい。 ただし SSL VPN のために、2 つの関連した AAA アトリビュート マッピングがあります:

AAA 属性名	SSL VPN 関連性
ユーザ VPN グループ	WebVPN コンテキストの下で定義されるポリシー グループへのマップ
webvpn コンテキスト	WebVPN 実際のコンテキストへのマップ自体

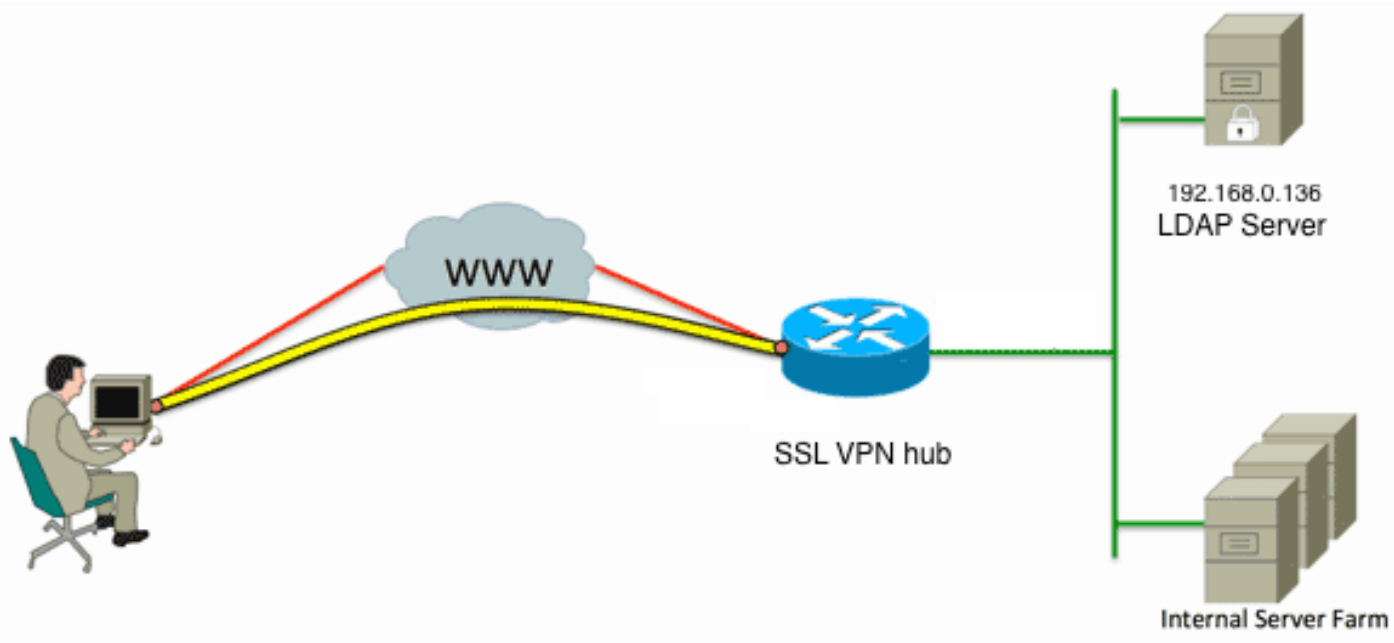
従ってどちらかに関連した LDAP アトリビュートをマッピング する LDAP アトリビュート マップ必要これら二つの AAA 属性の 1 つ。

設定

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup

Tool（登録ユーザ専用）を使用してください。

ネットワーク図



この設定は AAA アトリビュート ユーザ VPN グループに「memberOf」LDAP アトリビュートをマッピング するために LDAP アトリビュート マップを使用します。

1. 認証方式および AAAサーバグループを設定して下さい。

```
aaa new-model
!
!
aaa group server ldap AD
 server DC1
!
aaa authentication login default local
aaa authentication login vpn local
aaa authentication login AD group ldap local
aaa authorization exec default local
```

2. LDAP アトリビュート マップを設定して下さい。

```
ldap attribute-map ADMAP
 map type memberOf user-vpn-group
```

3. 前の LDAP アトリビュート マップを参照する LDAPサーバを設定して下さい。

```
ldap server DC1
 ipv4 192.168.0.136
 attribute map ADMAP
 bind authenticate root-dn CN=Cisco Systems,OU=Service Accounts,DC=chillsthrills,
DC=local password 7 <removed>
 base-dn DC=chillsthrills,DC=local
```

4. WebVPN サーバとして機能するためにルータを設定して下さい。 この例では、「memberOf」アトリビュートが「ユーザ VPN グループ」アトリビュートにマッピング されるので、WebVPN 単一 コンテキストは「NOACCESS」ポリシーを含む複数のポリシー グループで設定されます。 このポリシー グループは一致する「memberOf」値がないユーザのためです。

```
ip local pool vpnpool 192.168.200.200 192.168.200.250
!
webvpn gateway gateway_1
```

```
 hostname vpn
 ip address 173.11.196.220 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-2564112419
 logging enable
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-2.5.2019-k9.pkg sequence 1
 !
webvpn install csd flash:/webvpn/sdesktop.pkg
 !
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
  hide-url-bar
  timeout idle 60
  timeout session 1
 !
 !
 policy group CN=T,OU=MyBusiness,DC=chillsthrills,DC=local
  functions svc-enabled
  banner "special access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
   svc split include 192.168.0.0 255.255.255.0
   svc split include 10.10.10.0 255.255.255.0
   svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

警告

1. ユーザが「memberOf」複数のグループである場合、最初の「memberOf」値はルータによって使用されます。
2. この設定で異様である何がポリシー グループの名前が「memberOf 値」のための LDAPサーバによって押される**完全な**ストリングのための完全に一致するものでなければならないことです。 通常管理者はポリシー グループのためにより短く、より関連した名前を、VPNACCESS のような使用します、見かけ上の問題から離れてこれはより大きい問題を引き起こす場合があります。 使用された何がこの例で「memberOf」アトリビュート ストリングがかなり大きい珍しくないですより。 たとえば、このデバッグ メッセージを考慮して下さい:

```
ip local pool vpnpool 192.168.200.200 192.168.200.250
!
webvpn gateway gateway_1
 hostname vpn
 ip address 173.11.196.220 port 443
```

```
 http-redirect port 80
 ssl trustpoint TP-self-signed-2564112419
 logging enable
 inservice
 !
webvpn install svc flash:/webvpn/anyconnect-win-2.5.2019-k9.pkg sequence 1
 !
webvpn install csd flash:/webvpn/sdesktop.pkg
 !
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
  hide-url-bar
  timeout idle 60
  timeout session 1
 !
 !
 policy group CN=T,OU=MyBusiness,DC=chillsthrills,DC=local
  functions svc-enabled
  banner "special access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
   svc split include 192.168.0.0 255.255.255.0
   svc split include 10.10.10.0 255.255.255.0
   svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

AD から届くストリングは次のとおりであることを明らかに示します:

```
"CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,DC=chillsthrills,DC=local"
```

ただし、定義されるそのようなポリシー グループがないので管理者がそのようなグループ ポリシーを設定することを試みる場合 Cisco IOS にポリシー グループ名前で文字の数の制限があるのでエラーという結果に終ります:

```
"CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,DC=chillsthrills,DC=local"
```

そのような状況で 2 つの可能性のある 回避策があります:

1. 「部門」のような別の LDAP アトリビュートを、利用して下さい。この LDAP アトリビュート マップを考慮して下さい:

   ```
   "CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,DC=chillsthrills,DC=local"
   ```

   この場合ユーザ向けの部門 アトリビュートの値は VPNACCESS のような値に設定 することができ、WebVPN 設定は少しより簡単です:

   ```
   webvpn context VPNACCESS
    secondary-color white
    title-color #669999
    text-color black
    ssl authenticate verify all
    !
   ```

```
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
 !
 policy group VPNACCESS
  functions svc-enabled
  banner "access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
  svc split include 192.168.0.0 255.255.255.0
  svc split include 10.10.10.0 255.255.255.0
  svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

2. LDAP アトリビュート マップで DN にストリング キーワードを使用して下さい。前の回避策が適していない場合管理者は LDAP アトリビュート マップで「memberOf」ストリングからちょうど Common Name（CN）値を得るために dn にストリング キーワードを使用できます。 このシナリオで LDAP アトリビュート マップは次のとおりです:

```
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
 !
 policy group VPNACCESS
  functions svc-enabled
  banner "access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
  svc split include 192.168.0.0 255.255.255.0
  svc split include 10.10.10.0 255.255.255.0
  svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

そして WebVPN 設定は次のとおりです:

```
webvpn context VPNACCESS
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 policy group NOACCESS
```

```
  banner "Access denied per user group restrictions in Active Directory.
Please contact your system administrator or manager to request access."
 !
 policy group VPNACCESS
  functions svc-enabled
  banner "access-granted"
  svc address-pool "vpnpool"
  svc default-domain "cisco.com"
  svc keep-client-installed
  svc rekey method new-tunnel
  svc split dns "cisco.com"
  svc split include 192.168.0.0 255.255.255.0
  svc split include 10.10.10.0 255.255.255.0
  svc split include 172.16.254.0 255.255.255.0
  svc dns-server primary 192.168.0.136
 default-group-policy NOACCESS
 aaa authentication list AD
 gateway gateway_1
 inservice
!
end
```

注: 従って LDAPサーバから他のローカルで固有の値に届く値を一致するためにアトリビュート マップの下で **Map 値** コマンドを使用できる ASA でとは違って Cisco IOS ヘッドエンドにこのオプションがないし、適用範囲が広いようにないあります。 Cisco バグ ID CSCts31840 はこれを当たるためにファイルされました。

確認

ここでは、設定が正常に動作していることを確認します。

特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

- **show ldap attributes**
- **show ldap server all**

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

マッピング する LDAP アトリビュートを解決するためにこれらのデバッグを有効に して下さい:

- **debug ldap all**
- **debug ldap event**
- **debug aaa authentication**
- **debug aaa authorization**