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

内容

概要

このドキュメントでは、正しい VPN ポリシーをクレデンシャルに基づいてユーザに自動的に割り当てるために Lightweight Directory Access Protocol (LDAP) 属性マップを設定する方法について説明します。

> **注**：Cisco IOS®ヘッドエンドに接続するSecure Sockets Layer VPN(SSL VPN)ユーザのLDAP認証のサポートは、Cisco Bug ID CSCuj20940で追跡されます。サポートが正式に追加されるまで、LDAPサポートがががが最善です。

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。

- Cisco IOSでのSSL VPN
- 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いています。

- 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ました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

LDAPは、ベンダーに依存しないオープンな業界標準のアプリケーションプロトコルであり、インターネットプロトコル(IP)ネットワーク上で分散ディレクトリ情報サービスにアクセスし、維持します。ディレクトリサービスは、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において、ネットワーク全体でユーザ、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関する情報を共有できるため、重要な役割を果たします。

VPN ユーザには通常とは別のアクセス権限を与えたり、WebVPN コンテンツを提供したりすることを考える管理者は少なくありません。これは、VPNサーバ上のさまざまなVPNポリシーを設定し、クレデンシャルに応じてこれらのポリシーセットを各ユーザに割り当てることで完了できます。これは手動で実行できますが、ディレクトリサービスを使用してプロセスを自動化する方が効率的です。LDAPを使用してグループポリシーをユーザに割り当てるには、Active Directory(AD)属性「memberOf」などのLDAP属性をVPNヘッドエンドで認識される属性にマッピングするマップを設定する必要があります。

適応型セキュリティアプライアンス(ASA)では、『LDAP属性マップのASAの使用の設定例』に示すように、LDAP属性マップを持つ異なるユーザに異なるグループポリシーを割り当てることで、これが定期的に実現されます。

Cisco IOSでは、WebVPNコンテキストで異なるポリシーグループを設定し、LDAP属性マップを使用してユーザが割り当てられるポリシーグループを決定することで、同じことが実現できます。Cisco IOSヘッドエンドでは、「memberOf」AD属性がAuthentication, Authorization, and Accounting(AAA)属性サプリカントグループにマッピングされます。デフォルトの属性マッピングの詳細については、「ダイナミック属性マップを使用したIOSデバイスでのLDAPの設定例」を参照してください。ただし、SSL VPNでは、関連する2つのAAA属性マッピングがあります。

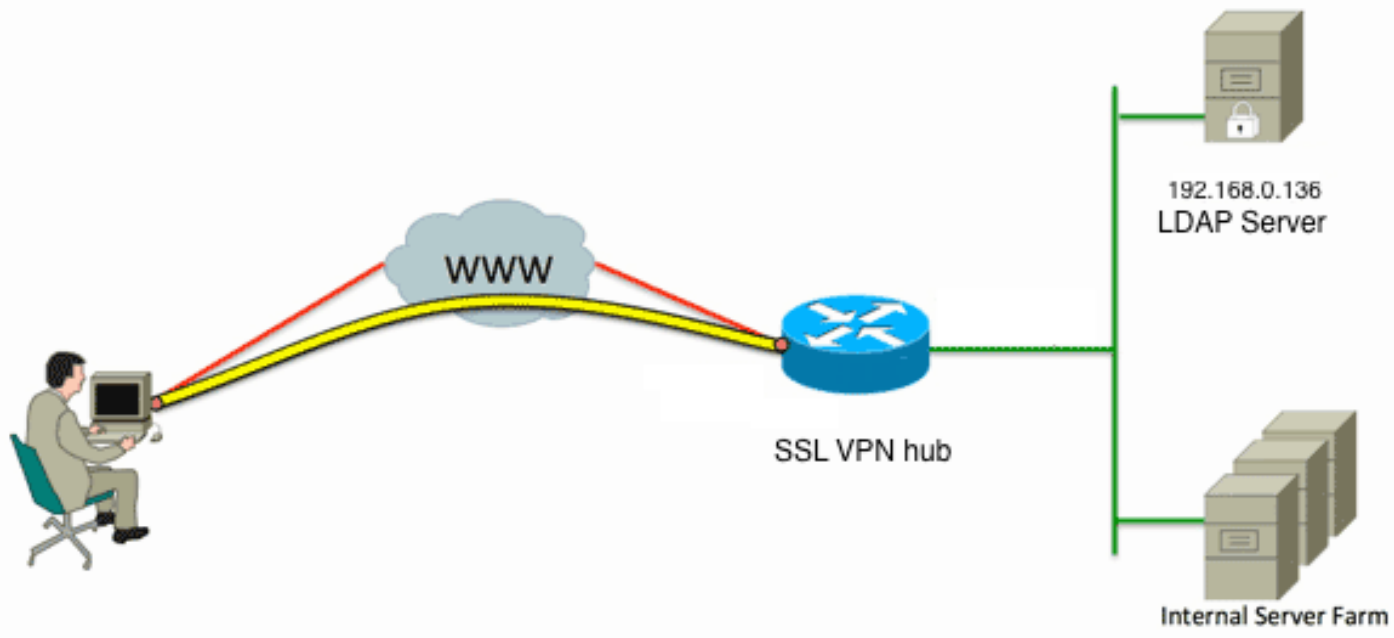
AAA属性名	SSL VPNの関連性
user-vpn-group	WebVPNコンテキストで定義されたポリシーグループへのマップ
webvpn-context	実際のWebVPNコンテキスト自体にマップする

したがって、LDAP属性マップは、関連するLDAP属性を、これら2つのAAA属性のいずれかにマッピングする必要があります。

設定

> **注**：このセクションで使用されるコマンドの詳細については、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



この設定では、LDAP属性マップを使用して、「memberOf」LDAP属性をAAA属性user-vpn-groupにマッピングします。

1. 認証方式とAAAサーバグループを設定します。

```
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属性マップを設定します。

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

3. 前のLDAP属性マップを参照するLDAPサーバを設定します。

```
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ようにルータを設定します。この例では、「memberOf」属性は「user-vpn-group」属性にマッピングされるため、単一のWebVPN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」値を持たないユーザを対象としています。

```
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. ユーザが複数のグループの「memberOf」の場合、最初の「memberOf」値がルータによって使用されます。
2. この設定で奇妙なのは、ポリシーグループの名前が、「memberOf値」に対してLDAPサーバによってプッシュされた完全な文字列と完全に一致している必要があることです。 通常、管理者はVPNACCESSなどのポリシーグループに対してより短い、より関連性の高い名前を使用しますが、表面的な問題とは別にこれが大きな問題につながる可能性があります。「memberOf」属性の文字列が、この例で使用されている文字列よりも大きくなることは珍しくありません。たとえば、次のデバッグメッセージについて考えます。

   ```
   004090: Aug 23 08:26:57.235 PCTime: %SSLVPN-6-INVALID_RADIUS_CONFIGURATION:
   Radius configured group policy "CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,
   DC=chillsthrills,DC=local" does not exist
   ```

   ADから受信した文字列が次のようになっていることを明確に示します。

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

   ただし、このようなポリシーグループが定義されていないため、管理者がこのようなグループポリシーを設定しようとすると、Cisco IOSのポリシーグループ名の文字数に制限があるため、エラーが発生します。

   ```
   HOURTR1(config-webvpn-context)#webvpn context VPNACCESS
   HOURTR1(config-webvpn-context)# policy group "CN=VPNACCESS,OU=Security Groups,
   ```

```
OU=MyBusiness,DC=chillsthrills,DC=local"
Error: group policy name cannot exceed 63 characters
```

このような状況では、2つの回避策があります。

1. 別のLDAP属性（「department」など）を使用します。次のLDAP属性マップを検討します。

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

この場合、ユーザのdepartment属性の値をVPNACCESSなどの値に設定でき、WebVPN設定は少し単純です。

```
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属性マップでDN-to-stringキーワードを使用します。前述の回避策が適切でない場合、管理者はLDAP属性マップでdn-to-stringキーワードを使用して、「memberOf」文字列からCommon Name(CN)値だけを抽出できます。このシナリオでは、LDAP属性マップは次のようになります。

```
ldap attribute-map ADMAP
 map type memberOf user-vpn-group format dn-to-string
```

また、WebVPNの設定は次のようになります。

```
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：LDAPサーバから受信した値を他のローカルで有効な値に一致させるために、属性マップの下で**map value**コマンドを使用できるASAとは異なり、Cisco IOSヘッドエンドにはこのオプションがないため、柔軟性がありません。これに対処するため[に、Cisco Bug ID](#) CSCts31840が登録されています。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

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

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

注：debug コマンドを使用する前に、「[デバッグ コマンドの重要な情報」を参照してください。](#)

LDAP属性マッピングをトラブルシューティングするには、次のデバッグを有効にします。

- **debug ldap all**
- **debug ldap event**
- **aaa 認証のデバッグ**
- **debug aaa authorization**