在Cisco IOS頭端上使用LDAP的AnyConnect客戶端的策略組分配配置示例

目錄

簡介

本文檔介紹如何配置輕量級目錄訪問協定(LDAP)屬性對映，以便根據使用者的憑據自動為使用者分配正確的VPN策略。

> **附註**：思科錯誤ID CSCuj20940會跟蹤對連線到Cisco IOS®頭端的安全套接字層VPN(SSL VPN)使用者的LDAP身份驗證支援。在正式新增支援之前，LDAP支援是最佳選擇。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco IOS上的SSL VPN
- Cisco IOS上的LDAP身份驗證
- 目錄服務

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CISCO881-SEC-K9
- Cisco IOS軟體，C880軟體(C880DATA-UNIVERSALK9-M)，版本15.1(4)M，版本軟體(fc1)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

LDAP是一種開放的、供應商中立的行業標準應用協定，用於通過Internet協定(IP)網路訪問和維護分散式目錄資訊服務。目錄服務在開發內聯網和Internet應用程式中發揮著重要作用，因為它們允許在整個網路中共用有關使用者、系統、網路、服務和應用程式的資訊。

通常，管理員希望為VPN使用者提供不同的訪問許可權或WebVPN內容。這可以通過在VPN伺服器上配置不同的VPN策略以及根據使用者的憑證將這些策略集分配給每個使用者來完成。雖然可以手動完成此操作，但使用目錄服務實現該過程的自動化更有效。為了使用LDAP為使用者分配組策略，您需要配置一個對映，該對映將LDAP屬性(如Active Directory(AD)屬性「memberOf」)對映到VPN頭端可以識別的屬性。

在Adaptive Security Appliance(ASA)上，這通常是通過將不同的組策略分配給具有LDAP屬性對映的不同使用者來實現的，如ASA使用LDAP屬性對映配置示例所示。

在Cisco IOS上，通過在WebVPN上下文中配置不同的策略組，並使用LDAP屬性對映來確定將分配給使用者的策略組，可以實現相同目的。在Cisco IOS頭端上，「memberOf」AD屬性被對映到身份驗證、授權和記帳(AAA)屬性請求方組。有關預設屬性對映的詳細資訊，請參閱使用動態屬性對映的IOS裝置上的LDAP配置示例。但是對於SSL VPN，有兩個相關的AAA屬性對映：

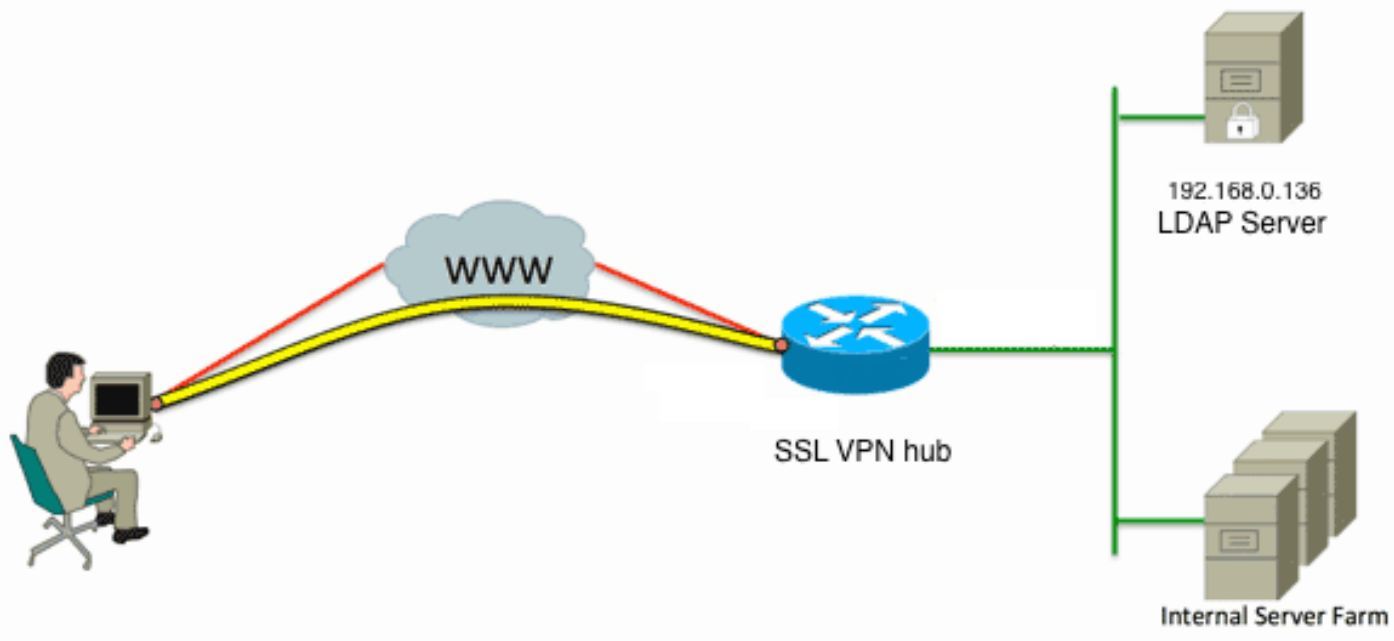
AAA屬性名稱	SSL VPN相關性
user-vpn-group	對映到在WebVPN上下文中定義的策略組
webvpn-context	對映到實際WebVPN上下文本身

因此，LDAP屬性對映需要將相關的LDAP屬性對映到這兩個AAA屬性中的任意一個。

設定

> **附註**：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖表



此配置使用LDAP屬性對映將「memberOf」LDAP屬性對映到AAA屬性user-vpn-group。

1. 配置身份驗證方法和AAA伺服器組。

```
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. 配置LDAP屬性對映。

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

3. 配置引用以前的LDAP屬性對映的LDAP伺服器。

```
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. 將路由器配置為充當WebVPN伺服器。在本示例中，由於「memberOf」屬性將對映到「user-vpn-group」屬性，因此為單個WebVPN上下文配置多個策略組，這些策略組包括「NOACCESS」策略。此策略組適用於沒有匹配「memberOf」值的使用者。

```
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
```

注意事項

1. 如果使用者是多個組的「memberOf」，則路由器使用第一個「memberOf」值。
2. 此配置中的奇怪之處在於，策略組的名稱必須與LDAP伺服器推送的memberOf value的完整字串完全匹配。 通常，管理員會為策略組使用較短且更相關的名稱，如VPNACCESS，但是除了修飾問題之外，這可能會導致更大的問題。「memberOf」屬性字串比本示例中使用的字串大得多並非罕見。例如，請考慮以下偵錯訊息：

   ```
   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
   ```

   它清楚地顯示，從AD接收的字串為：

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

   但是，由於沒有定義這樣的策略組，如果管理員嘗試配置這樣的組策略，則會導致錯誤，因為Cisco IOS對策略組名稱中的字元數有限制：

   ```
   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
   ```

在這種情況下，有兩種可能的解決方法：

1. 使用不同的LDAP屬性，如「department」。請考慮此LDAP屬性對映：

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

   在這種情況下，使用者的department屬性的值可設定為VPNACCESS之類的值，而WebVPN組態會更簡單：

```
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. 在LDAP屬性對映中使用DN-to-string關鍵字。如果上述解決方法不適用，則管理員可以在LDAP屬性對映中使用dn-to-string關鍵字，以便從「memberOf」字串中僅提取公用名(CN)值。在此方案中，LDAP屬性對映為：

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

WebVPN配置將是：

```
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
```

附註：在ASA中，可以在屬性對映下使用**map value**命令，以便將從LDAP伺服器接收的值與某個其他本地重要值相匹配，但與ASA不同，Cisco IOS頭端沒有此選項，因此不夠靈活。解決此問題的思科錯誤ID CSCts31840已失敗。

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用輸出直譯器工具來檢視**show**命令輸出的分析。

- **顯示ldap屬性**
- **show ldap server all**

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

附註：使用 **debug 指令之前，請先參閱**有關 Debug 指令的重要資訊。

為了對LDAP屬性對映進行故障排除，請啟用以下調試：

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