# Esempio di configurazione dell'assegnazione di gruppi di criteri per i client AnyConnect che usano LDAP sugli headend Cisco IOS

## Sommario



## Introduzione

In questo documento viene descritto come configurare le mappe di attributi LDAP (Lightweight Directory Access Protocol) in modo da assegnare automaticamente a un utente il criterio VPN corretto in base alle credenziali.

> **Nota:** Il supporto per l'autenticazione LDAP per gli utenti VPN SSL (Secure Sockets Layer) che si connettono a un headend Cisco IOS® viene registrato dall'ID bug Cisco CSCuj20940. Fino a quando il supporto non viene aggiunto ufficialmente, il supporto LDAP è la soluzione migliore.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SSL VPN su Cisco IOS
- Autenticazione LDAP su Cisco IOS
- Servizi directory

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CISCO 881-SEC-K9
- Software Cisco IOS, software C880 (C880DATA-UNIVERSALK9-M), versione 15.1(4)M, SOFTWARE RELEASE (fc1)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Il protocollo LDAP è un protocollo di applicazione standard del settore aperto, indipendente dal fornitore, per l'accesso e la gestione di servizi di directory distribuiti su una rete IP (Internet Protocol). I servizi di elenchi in linea svolgono un ruolo importante nello sviluppo delle applicazioni Intranet e Internet in quanto consentono la condivisione di informazioni su utenti, sistemi, reti, servizi e applicazioni in tutta la rete.

Spesso gli amministratori desiderano fornire agli utenti VPN autorizzazioni di accesso diverse per il contenuto WebVPN. A tale scopo, è possibile configurare criteri VPN diversi nel server VPN e assegnare tali set di criteri a ogni utente in base alle credenziali. Sebbene sia possibile completare questa operazione manualmente, è più efficiente automatizzare il processo con i servizi directory. Per utilizzare LDAP per assegnare un criterio di gruppo a un utente, è necessario configurare una mappa che esegua il mapping di un attributo LDAP, ad esempio l'attributo di Active Directory (AD) "memberOf", a un attributo riconosciuto dall'headend VPN.

Sull'appliance ASA (Adaptive Security Appliance), questo obiettivo viene regolarmente raggiunto tramite l'assegnazione di criteri di gruppo diversi a utenti diversi con una mappa degli attributi LDAP, come mostrato nell'esempio di configurazione dell'uso delle mappe di attributi LDAP da parte dell'ASA.

Su Cisco IOS, lo stesso risultato può essere ottenuto con la configurazione di diversi gruppi di criteri nel contesto WebVPN e l'uso di mappe di attributi LDAP per determinare quale gruppo di criteri verrà assegnato all'utente. Sugli headend Cisco IOS, l'attributo "memberOf" di Active Directory è mappato al supplicant-group dell'attributo Authentication, Authorization, and Accounting (AAA). Per ulteriori informazioni sui mapping di attributi predefiniti, vedere Esempio di configurazione di LDAP su dispositivi IOS che utilizzano mappe di attributi dinamici. Tuttavia, per la VPN SSL, sono disponibili due mapping di attributi AAA rilevanti:

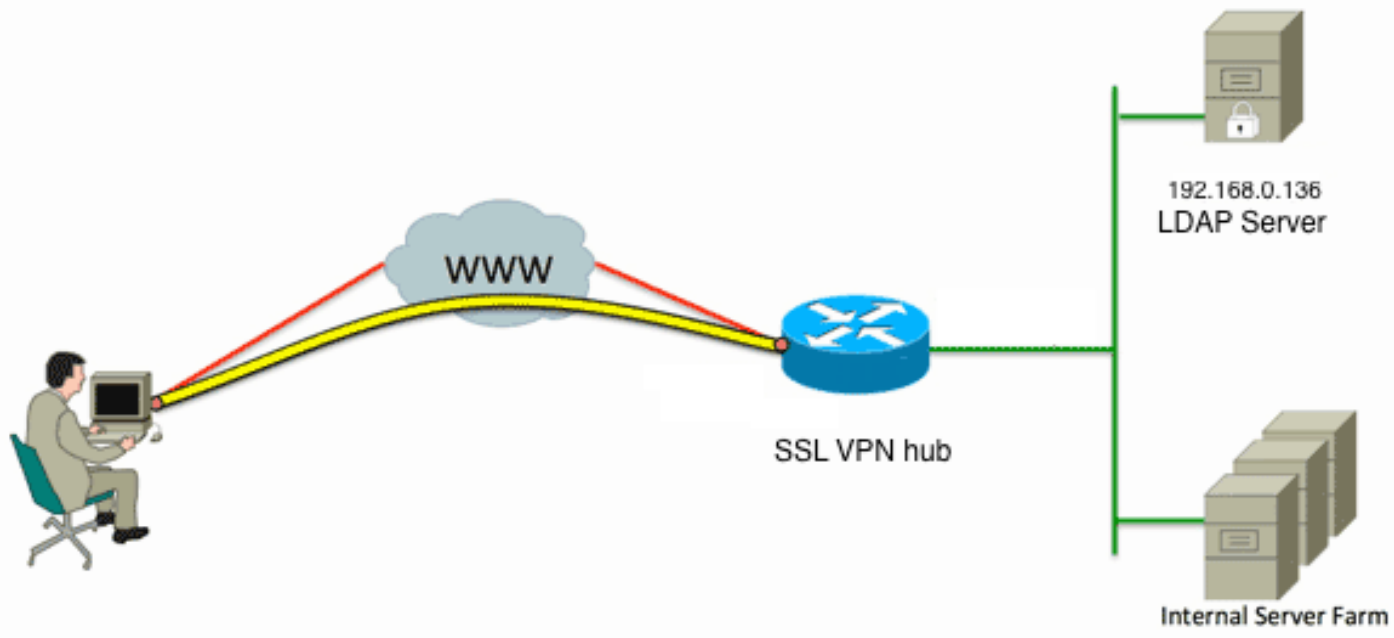
| Nome attributo AAA | Rilevanza VPN SSL |
|---|---|
| user-vpn-group | esegue il mapping al gruppo di criteri definito nel contesto WebVPN |
| webvpn-context | esegue il mapping al contesto WebVPN effettivo |

Pertanto, la mappa degli attributi LDAP deve mappare l'attributo LDAP rilevante a uno di questi due attributi AAA.

# Configurazione

**Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

## Esempio di rete




Questa configurazione utilizza una mappa degli attributi LDAP per mappare l'attributo LDAP "memberOf" all'attributo AAA user-vpn-group.

1. Configurare il metodo di autenticazione e il gruppo di server AAA.
```
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. Configurare una mappa attributi LDAP.
```
ldap attribute-map ADMAP
 map type memberOf user-vpn-group
```
3. Configurare il server LDAP che fa riferimento alla mappa attributi LDAP precedente.
```
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. Configurare il router in modo che agisca come server WebVPN. In questo esempio, poiché l'attributo "memberOf" verrà mappato all'attributo "user-vpn-group", viene configurato un singolo contesto WebVPN con più gruppi di criteri che includono un criterio "NOACCESS". Questo gruppo di criteri è destinato agli utenti che non dispongono di un valore "memberOf"

corrispondente.

```
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
```

## Avvertenze

1. Se l'utente è un "memberOf" a più gruppi, il router utilizza il primo valore "memberOf".
2. Ciò che è strano in questa configurazione è che il nome del gruppo di criteri deve corrispondere esattamente alla stringa **completa** sottoposta a push dal server LDAP per il "valore memberOf". Di solito gli amministratori utilizzano nomi più brevi e più pertinenti per il gruppo di criteri, ad esempio VPNACCESS, ma a parte il problema estetico, questo può portare a un problema più grande. Non è raro che la stringa dell'attributo "memberOf" sia notevolmente più grande di quella utilizzata in questo esempio. Ad esempio, considerare questo messaggio di debug:

```
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
```

La stringa ricevuta da AD è chiaramente la seguente:

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

Tuttavia, poiché tale gruppo di criteri non è stato definito, se l'amministratore tenta di configurare i criteri di gruppo di questo tipo, viene generato un errore perché Cisco IOS ha un limite al numero di caratteri nel nome del gruppo di criteri:

```
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
```

In tali situazioni esistono due possibili soluzioni:

1. Utilizzare un attributo LDAP diverso, ad esempio "reparto".Si consideri la seguente mappa attributi LDAP:

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

In questo caso, il valore dell'attributo department di un utente può essere impostato su un valore come VPNACCESS e la configurazione WebVPN è un po' più semplice:

```
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. Utilizzare la parola chiave DN-to-string nella mappa degli attributi LDAP.Se la soluzione precedente non è appropriata, l'amministratore può utilizzare la parola chiave dn-stringa nella mappa dell'attributo LDAP per estrarre solo il valore del nome comune (CN) dalla stringa "memberOf". In questo scenario, la mappa degli attributi LDAP sarebbe:

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

E la configurazione WebVPN sarebbe:

```
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
```

**Nota:** A differenza delle appliance ASA, in cui è possibile usare il comando **map value** in una mappa degli attributi per associare il valore ricevuto dal server LDAP a un altro valore localmente significativo, gli headend Cisco IOS non dispongono di questa opzione e non sono quindi così flessibili. Per risolvere questo problema, consultare l'ID bug Cisco CSCts31840.

# Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

- **mostra attributi ldap**
- **mostra tutto il server ldap**

# Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

**Nota:** consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.**

Per risolvere i problemi relativi alla mappatura degli attributi LDAP, abilitare i seguenti debug:

- **debug ldap all**
- **debug evento ldap**
- **debug autenticazione aaa**

- autorizzazione debug aaa