# تعيين مجموعة السياسات لعملاء AnyConnect الذين يستخدمون LDAP على مثال تكوين نهايات الاستقبال والبث الرئيسية من Cisco IOS

## المحتويات



## المقدمة

يوضح هذا المستند كيفية تكوين خرائط سمات البروتوكول الخفيف للوصول إلى الدليل (LDAP) لتعيين سياسة VPN الصحيحة تلقائيا إلى مستخدم استنادا إلى بيانات الاعتماد الخاصة به.

**ملاحظة**: يتم تعقب دعم مصادقة LDAP لمستخدمي طبقة مآخذ التوصيل الآمنة SSL VPN) VPN) الذين يقومون بالاتصال بوحدة الاستقبال والبث من Cisco IOS® بواسطة معرف تصحيح الأخطاء من Cisco CSCuj20940. إلى أن تتم إضافة الدعم رسميا، فإن دعم LDAP هو أفضل جهد.

## المتطلبات الأساسية

### المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- SSL VPN على Cisco IOS
- مصادقة LDAP على Cisco IOS
- خدمات الدليل

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco 881-SEC-K9
- برنامج Cisco IOS، برنامج C880 (C880DATA-universalk9-M)، الإصدار 15.1(4)M، برنامج الإصدار (FC1)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## معلومات أساسية

LDAP هو بروتوكول تطبيق مفتوح ومحايد من حيث المورد ومعياري في الصناعة للوصول إلى خدمات معلومات الدليل الموزعة وصيانتها عبر شبكة بروتوكول الإنترنت (IP). تؤدي خدمات الدليل دورا هاما في تطوير تطبيقات الإنترانت والإنترنت لأنها تتيح تبادل المعلومات عن المستخدمين، والأنظمة، والشبكات، والخدمات، والتطبيقات عبر الشبكة.

يريد المسؤولون بشكل متكرر تزويد مستخدمي VPN بأذونات وصول مختلفة أو محتوى WebVPN. ويمكن إكمال هذا الأمر بتكوين نهج VPN مختلفة على خادم الشبكة الخاصة الظاهرية (VPN) وتعيين مجموعات السياسات هذه لكل مستخدم وفقا لبيانات الاعتماد الخاصة به. وفي حين يمكن إكمال ذلك يدويا، إلا أنه من الأكثر فعالية أتمتة العملية بواسطة "خدمات الدليل". لاستخدام LDAP لتعيين سياسة مجموعة لمستخدم، يلزمك تكوين خريطة تقوم بتعيين سمة LDAP مثل سمة "memberOf" ل AD (Active Directory) لسمة يتم فهمها بواسطة وحدة الاستقبال والبث الخاصة بالشبكة الخاصة الظاهرية (VPN).

في جهاز الأمان القابل للتكيف (ASA)، يتم تحقيق ذلك بشكل منتظم من خلال تعيين سياسات مجموعات مختلفة لمستخدمين مختلفين مع خريطة سمة LDAP كما هو موضح في مثال تكوين إستخدام ASA لخرائط سمات LDAP.

على برنامج Cisco IOS، يمكن تحقيق نفس الشيء مع تكوين مجموعات السياسات المختلفة ضمن سياق WebVPN واستخدام خرائط سمات LDAP لتحديد مجموعة النهج التي سيتم تعيين المستخدم لها. في نهايات عنوان Cisco IOS، يتم تعيين سمة "memberOf" AD على مجموعة مسبب السمة المصادقة والتفويض والمحاسبة (AAA). لمزيد من التفاصيل حول تعيينات السمات الافتراضية، راجع LDAP على أجهزة IOS باستخدام مثال تكوين خرائط السمات الديناميكية. ومع ذلك بالنسبة لشبكة VPN الخاصة ب SSL، هناك تعيينان ذوي صلة لسمة AAA:

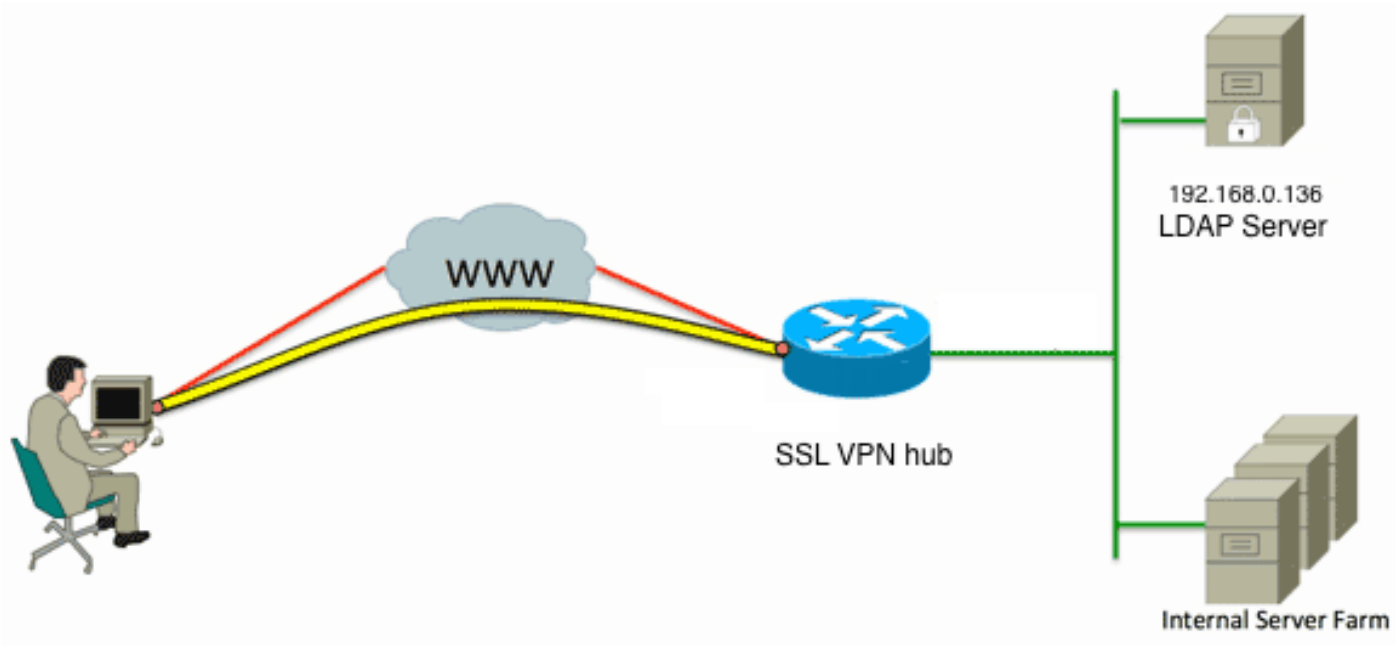
| اسم سمة AAA | صلة SSL VPN |
|---|---|
| user-vpn-group | تعيين إلى مجموعة النهج المعرفة ضمن سياق WebVPN |
| سياق WebVPN | خرائط لسياق WebVPN الفعلي نفسه |

لذلك يحتاج تعيين سمة LDAP إلى تعيين سمة LDAP ذات الصلة إلى إحدى سمتي AAA هاتين.

## التكوين

**ملاحظة**: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

## الرسم التخطيطي للشبكة




يستخدم هذا التكوين مخطط سمة LDAP لتعيين سمة LDAP "memberOf" إلى سمة AAA user-vpn-group.

1. قم بتكوين أسلوب المصادقة ومجموعة خوادم 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. تكوين تعيين سمة LDAP.

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

3. قم بتكوين خادم LDAP الذي يشير إلى تعيين سمة LDAP السابق.

```
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. قم بتكوين الموجه ليعمل كخادم WebVPN. في هذا المثال، نظرا لأنه سيتم تعيين السمة "memberOf" على السمة "user-vpn-group"، يتم تكوين سياق WebVPN واحد باستخدام مجموعات نهج متعددة تتضمن نهج "NOACCESS". مجموعة النهج هذه خاصة بالمستخدمين الذين ليس لديهم قيمة "memberOf" متطابقة.

```
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
```

## كافيتس

1. إذا كان المستخدم عبارة عن مجموعات متعددة "memberOf"، فسيتم إستخدام القيمة الأولى "memberOf" بواسطة الموجه.
2. الغريب في هذا التكوين هو أن اسم مجموعة السياسات يجب أن يكون مطابقا تماما للسلسلة **الكاملة** التي تم دفعها بواسطة خادم LDAP ل "memberOf value". عادة ما يستخدم المسؤولون أسماء أقصر وأكثر صلة بمجموعة السياسات، مثل VPNaccess، ولكن بغض النظر عن قضية التجميل، يمكن أن يؤدي ذلك إلى مشكلة أكبر. ليس من غير الشائع أن تكون سلسلة السمة "memberOf" أكبر بكثير مما تم إستخدامه في هذا المثال.
على سبيل المثال، تأمل في رسالة تصحيح الأخطاء هذه:
```
:Aug 23 08:26:57.235 PCTime: %SSLVPN-6-INVALID_RADIUS_CONFIGURATION :004090
,Radius configured group policy "CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness
DC=chillsthrills,DC=local" does not exist
```
وهو يظهر بوضوح ان السلسلة المتلقاة من AD هي:
```
"CN=VPNACCESS,OU=SecurityGroups,OU=MyBusiness,DC=chillsthrills,DC=local"
```
ومع ذلك، نظرا لعدم وجود مجموعة نهج محددة من هذا القبيل، إذا حاول المسؤول تكوين نهج المجموعة هذا، فإنه يؤدي إلى حدوث خطأ لأن Cisco IOS لديه حد على عدد الأحرف في اسم مجموعة النهج:
```
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
```
وفي مثل هذه المواقف هناك حلان محتملان:

1. أستخدم سمة LDAP مختلفة، مثل "department".ضع في الاعتبار تعيين سمة LDAP هذا:

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

في هذه الحالة، يمكن تعيين قيمة سمة القسم لمستخدم على قيمة مثل VPNaccess وتكوين WebVPN أبسط قليلا:

```
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. أستخدم الكلمة الأساسية DN إلى سلسلة في تعيين سمة LDAP.إذا كان الحل السابق غير مناسب، فيمكن حينئذ للمسؤول إستخدام الكلمة الأساسية dn-to-string في خريطة سمة LDAP لاستخراج قيمة الاسم المشترك (CN) فقط من السلسلة "memberOf". في هذا السيناريو، تكون خريطة سمة LDAP:

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

وسيكون تكوين WebVPN:

```
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
```

**ملاحظة**: بخلاف الموجود في ASAs حيث يمكنك إستخدام الأمر **map value** تحت خريطة سمة لمطابقة القيمة المستلمة من خادم LDAP إلى قيمة أخرى ذات قيمة محلية، لا تحتوي رؤوس Cisco IOS على هذا الخيار وبالتالي فإنها لا تكون مرنة. تم تصنيف معرف تصحيح الأخطاء من CSCts31840 Cisco من أجل معالجة هذا الأمر.

## التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

- **إظهار سمات ldap**
- **show ldap server all**

## استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

**ملاحظة**: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

لاستكشاف أخطاء تعيين سمة LDAP وإصلاحها، قم بتمكين عمليات تصحيح الأخطاء التالية:

- **debug ldap all**
- **حدث debug ldap**
- **تصحيح أخطاء مصادقة aaa (المصادقة والتفويض والمحاسبة)**
- **تخويل debug aaa**

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).