إستخدام مثال تكوين خرائط سمات LDAP

المحتويات

المقدمة
الإجراء
وضع مستخدمي LDAP في نهج مجموعة محدد (مثال عام)
تكوين نهج مجموعة NOACCESS
تنفيذ سياسة السمات المستندة إلى مجموعة (مثال)
فرض Active Directory لـ "تعيين عنوان IP ثابت" لأنفاق IPsec و SVC
تطبيق Active Directory لـ "طلب إذن الوصول عن بعد، السماح/رفض الوصول"
تطبيق Active Directory لـ "عضوية المجموعة للسماح بالوصول أو رفضه"/"عضوية المجموعة للسماح بالوصول أو رفضه"
فرض Active Directory لـ "تسجيل الدخول لتواريخ/أوقات السماح"
أستخدم تكوين خريطة LDAP لتعيين مستخدم في نهج مجموعة محدد واستخدام الأمر authorization-server-group، في حالة المصادقة المزدوجة
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
تصحيح أخطاء حركة LDAP
تعذر على ASA مصادقة المستخدمين من خادم LDAP

المقدمة

يوضح هذا المستند الكيفية التي يمكن بها تعيين أي سمة من سمات Microsoft/AD على سمة Cisco.

الإجراء

1. في خادم Active Directory (AD)/Lightweight Directory Access Protocol (LDAP):أختر **user1**.انقر بزر الماوس الأيمن فوق **خصائص >** أختر علامة تبويب ليتم إستخدامها لتعيين سمة (على سبيل المثال، علامة تبويب عام).أختر حقل/سمة، على سبيل المثال، حقل Office، ليتم إستخدامه لفرض النطاق الزمني، أو لخذ نص الشعار (على سبيل المثال، مرحبا بك في LDAP !!!). يتم تخزين تكوين Office على واجهة المستخدم الرسومية في سمة AD/LDAP physicalDeliveryOfficeName.
2. في جهاز الأمان القابل للتكيف (ASA)، وهو أجل إنشاء جدول تعيين سمة LDAP، قم بتعيين سمة AD/LDAP physicalDeliveryOfficeName إلى شعار سمة ASA1:

```
B200-54(config)# show run ldap
ldap attribute-map Banner
map-name physicalDeliveryOfficeName Banner1
```

3. أربط خريطة سمة LDAP بإدخال AAA-server:

```
B200-54(config-time-range)# show runn aaa-server microsoft
aaa-server microsoft protocol ldap
aaa-server microsoft host audi-qa.frdevtestad.local
ldap-base-dn dc=frdevtestad,dc=local
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password hello
```

```
ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
ldap-attribute-map Banner
```

4. قم بإنشاء جلسة عمل للوصول عن بعد وتحقق من تدقيق الشعار مرحبا به إلى LDAP !!!! إلى مستخدم شبكة VPN.

وضع مستخدمي LDAP في نهج مجموعة محدد (مثال عام)

ويوضح هذا المثال استخدام المستخدمين الصادقة على خادم AD-LDAP 1 ويسترجع قيمة حقل القسم حتى يمكن تعيينها إلى نهج مجموعة ASA/PIX يمكن فرض السياسات منها.

1. على خادم AD/LDAP:اختر **user1**.انقر بزر الماوس الأيمن > **خصائص**.اختر علامة تبويب المؤسسة).اختر سمة لتعيين استخدامها يتم (على سبيل المثال، علامة تبويب المؤسسة).اختر سمة/حقل، على سبيل المثال، القسم، يتم استخدامه لفرض سياسة المجموعة، وأدخل قيمة نهج المجموعة (Group-Policy1) على ASA/PIX. يتم تخزين تكوين الإدارة على واجهة المستخدم الرسومية في قسم سمة AD/LDAP.
2. تحديد جدول ldap-attribute-map.

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department Group-Policy
5520-1(config)#
```

3. قم بتحديد group-policy و group_policy1 على الجهاز وسمات النهج المطلوبة.
4. قم بإنشاء نفق الوصول عن بعد لشبكة VPN وتحقق من أن جلسة العمل ترث السمات من Group-Policy1 (وأي سمات أخرى قابلة للتطبيق من نهج المجموعة الافتراضي).
ملاحظة: إضافة المزيد من السمات إلى الخريطة حسب الحاجة. يوضح هذا المثال الحد الأدنى فقط للتحكم في هذه الوظيفة المحددة (وضع مستخدم في نهج مجموعة ASA/PIX 7.1.x محدد). يوضح المثال الثالث هذا النوع من الخرائط.

تكوين نهج مجموعة NOACCESS

يمكنك إنشاء نهج مجموعة NOACCESS لرفض اتصال VPN عندما لا يكون المستخدم جزءا من أي من مجموعات LDAP. يتم عرض قصاصة التكوين هذه للمرجع الخاص بك:

```
group-policy NOACCESS internal
group-policy NOACCESS attributes
vpn-simultaneous-logins 0
vpn-tunnel-protocol IPSec webvpn
```

يجب تطبيق نهج المجموعة هذا كنهج مجموعة افتراضي على مجموعة النفق. وهذا يسمح للمستخدمين الذين يحصلون على تعيين من خريطة سمة LDAP، على سبيل المثال، أولئك الذين ينتمون إلى مجموعة LDAP مرغوبة، بالحصول على سياسات المجموعة المطلوبة الخاصة بهم، والمستخدمين الذين لا يحصلون على أي تعيين، على سبيل المثال، أولئك الذين لا ينتمون إلى أي من مجموعات LDAP المطلوبة، للحصول على نهج مجموعة NOACCESS من مجموعة النفق، التي تمنع الوصول إليهم.

تلميح: نظرا لأنه قد تم تعيين سمة عمليات تسجيل الدخول المتزامنة ل VPN على 0 هنا، يجب تعريفها بشكل صريح في جميع سياسات المجموعة الأخرى أيضا؛ وإلا، يمكن توريثها من نهج المجموعة الافتراضي لمجموعة النفق تلك، والذي هو في هذه الحالة نهج NOACCESS.

تنفيذ سياسة السمات المستندة إلى مجموعة (مثال)

1. على خادم AD-LDAP، موقع Active Directory Users and Computers بإعداد سجل مستخدم (VPNUserGroup) لمثيل مجموعة يتم فيها تكوين سمات VPN.
2. على خادم AD-LDAP، موقع Active Directory Users and Computers بتعريف حقل Department لكل سجل مستخدم للإشارة إلى سجل المجموعة (VPNUserGroup) في الخطوة 1. اسم المستخدم في هذا المثال هو web1. **ملاحظة**: لم يتم إستخدام سمة AD في الواقع، يمكن. المجموعة إلى نهج إيقاع منطقي يشير قسم لأن القسم إلا في إستخدام أي مجال. المطلب هو أن هذا الحقل يجب تعيينه إلى نهج مجموعة سمات VPN من Cisco كما هو موضح في هذا المثال.
3. تحديد جدول LDAP-attribute-map:

   ```
   5520-1(config)# show runn ldap
   ldap attribute-map Our-AD-Map
   map-name department IETF-Radius-Class
   map-name description\Banner1
   map-name physicalDeliveryOfficeName IETF-Radius-Session-Timeout
   5520-1(config)#
   ```

   يتم AD-LDAP، الوصف و Office، (يمثلهما وصف أسماء AD و PhysicalDeliveryOfficeName) هما سمتان سجل المجموعة (ل VPNUSerGroup) اللتان تخترعان إلى شعار شعار سمات VPN من Cisco1 و IETF-Radius-Session-Timeout.سمة القسم خاصة بسجل المستخدم للتعيين إلى اسم نهج المجموعة الخارجي على ASA (VPNUSer)، والذي يقوم بعد ذلك بالتعيين مرة أخرى إلى سجل VPNuserGroup على خادم AD-LDAP، حيث يتم تعريف السمات.**ملاحظة**: يجب تعريف سمة Cisco (Group-Policy) في مخطط سمة LDAP. يمكن أن تكون سمة AD المعينة الخاصة بها أي سمة AD قابلة للتعيين. يستخدم هذا المثال قسم لأنه أكثر الأسماء منطقية التي تشير إلى نهج المجموعة.
4. قم بتكوين خادم AAA باستخدام اسم خريطة سمة LDAP الذي سيتم إستخدامه لعمليات مصادقة LDAP والتخويل والمحاسبة (AAA):

   ```
   5520-1(config)# show runn aaa-server LDAP-AD11
   aaa-server LDAP-AD11 protocol ldap
   aaa-server LDAP-AD11 host 10.148.1.11
   ldap-base-dn cn=Users,dc=nelson,dc=cisco,dc=com
   ldap-scope onelevel
   ldap-naming-attribute sAMAccountName
   ldap-login-password altiga
   ldap-login-dn cn=Administrator,cn=Users,dc=nelson,dc=cisco,dc=com
   ldap-attribute-map Our-AD-Map
   5520-1(config)#
   ```

5. قم بتحديد مجموعة أنفاق باستخدام مصادقة LDAP أو تفويض LDAP. مثال مصادقة LDAP. تنفيذ المصادقة + (التخويل) تنفيذ نهج السمة إذا تم تعريف السمات.

   ```
   5520-1(config)# show runn tunnel-group
   remoteAccessLDAPTunnelGroup
   tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
   authentication-server-group LDAP-AD11
   accounting-server-group RadiusACS28
   5520-1(config)#
   ```

   مثال على تفويض LDAP. التكوين المستخدم للشهادات الرقمية.

   ```
   5520-1(config)# show runn tunnel-group
   remoteAccessLDAPTunnelGroup
   tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
   authentication-server-group none
   authorization-server-group LDAP-AD11
   accounting-server-group RadiusACS28
   authorization-required
   ```

```
authorization-dn-attributes ea
5520-1(config)#
```

6. تحديد سياسة مجموعة خارجية. اسم نهج المجموعة هو قيمة سجل مستخدم AD-LDAP الذي يمثل المجموعة (VPNUserGroup).
```
5520-1(config)# show runn group-policy VPNUserGroup
group-policy VPNUserGroup external server-group LDAP-AD11
5520-1(config)#
```
7. قم بإنشاء النفق والتحقق من فرض السمات. في هذه الحالة، يتم فرض الشعار و Session-Timeout من سجل VPNuserGroup على الإعلان.

فرض Active Directory ل "تعيين عنوان IP ثابت" لأنفاق IPsec و SVC

سمة AD هي msRADIOramedIPAddress. يتم تكوين السمة في خصائص مستخدم AD، علامة التبويب طلب اتصال، تعيين عنوان IP ثابت.

فيما يلي الخطوات:

1. في خادم AD، ضمن خصائص المستخدم، علامة التبويب طلب اتصال، قم بتعيين عنوان IP ثابت، أدخل قيمة عنوان IP للتعيين إلى جلسة عمل IPsec/SVC (10.20.30.6).
2. في ASA، قم بإنشاء ldap-attribute-map بهذا التعيين:
```
5540-1# show running-config ldap
ldap attribute-map Assign-IP
map-name msRADIUSFramedIPAddress IETF-Radius-Framed-IP-Address
5540-1#
```
3. على ASA، تحقق من تكوين تعيين عنوان VPN لتضمين vpn-addr-assign-aaa:
```
5520-1(config)# show runn all vpn-addr-assign
vpn-addr-assign aaa
no vpn-addr-assign dhcp
vpn-addr-assign local
5520-1(config)#
```
4. قم بإنشاء جلسات عمل السلطة عن بعد (RA) لـ IPsec/SVC وتحقق من عرض vpn-sessionDB عن بعد|svc أن حقل IP المعين صحيح (10.20.30.6).

تطبيق Active Directory ل "طلب إذن الوصول عن بعد، السماح/رفض الوصول"

يدعم جميع جلسات الوصول عن بعد إلى شبكة VPN: IPSec، WebVPN، و SVC. يحتوي "السماح بالوصول" على قيمة TRUE. قيمة FALSE الخاصة بـ DENY Access. اسم سمة AD هو msNPAllowDialin.

يوضح هذا المثال إنشاء خريطة LDAP-attribute-map التي تستخدم بروتوكولات Cisco Tunneling-Protocols لإنشاء شروط السماح بالوصول (TRUE) والرفض (FALSE). على سبيل المثال، إذا تم تعيين tunnel-protocol=L2TPover IPsec (8)، فيمكن إنشاء حالة FALSE إذا حاولت فرض الوصول إلى WebVPN و IPsec. ويتطابق المنطق العكسي أيضا.

فيما يلي الخطوات:

1. في خصائص مستخدم خادم AD1، اطلب الدخول، أخترت السماح بالوصول المناسب وأ رفض وصول كل مستخدم. **ملاحظة**: إذا أخترت الخيار الثالث، التحكم في الوصول من خلال نهج الوصول عن بعد، فإن الأذونات التي يتم إرجاعها من خادم AD، لذلك يتم فرضها تستند إلى إعداد نهج المجموعة الداخلي لـ ASA/PIX'.
2. في ASA، قم بإنشاء ldap-attribute-map بهذا التعيين:
```
ldap attribute-map LDAP-MAP
map-name msNPAllowDialin Tunneling-Protocols
```

```
map-value msNPAllowDialin FALSE 8
map-value msNPAllowDialin TRUE 20
5540-1#
```

ملاحظة: إضافة المزيد من السمات إلى الخريطة حسب الحاجة. يوضح هذا المثال الحد الأدنى للتحكم في هذه الوظيفة المحددة (السماح بالوصول أو رفضه استنادا إلى ldap؟msNPAllowDialin سمة خريطة تعرض أو تعين ما إذا (يفتاهالا بلطلا دادعإ). يتم تعيين شرط القيمة الخطأ إلى بروتوكول FALSE 8رفض الوصول لمستخدم 1. يتم تعيين شرط القيمة (8) إلى نفق L2TPoverIPsec، يتم . 2 للمستخدم الوصول بالسماح. (القيمة 20) يفشل نفق بروتوكول WebVPN + IPsec إلى القيمة الحقيقية. قد يفشل AD، بسبب عدم تطابق AD على 1 مستخدم كمستخدم مصادقته تمت الذي WebVPN/IPsec، مستخدم بسبب فشل بروتوكول النفق. L2TPoverIPsec، كمستخدم 1 على AD، تصادم القاعدة بسبب فشل AD على user2 ك مصادقته تمت الذي WebVPN/IPsec، مستخدم سيتجح الرفض. (السماح AD، على user2 ك تصادم L2TPoverIPsec، (تطابق النفق بروتوكول + القاعدة بالبالسيس عدم تطابق بروتوكول النفق.

بسبب فشل بروتوكول النفق، كما هو محدد في RFCs 2867 و 2868.

تطبيق Active Directory ل "وضع/وضعية المجموعة" للسماح بالوصول أو رفضه

ترتبط هذه الحالة ارتباطا وثيقا بالحالة 5، وتوفر تدفقا أكثر منطقية، وهي الطريقة الموصى بها، حيث أنها تحدد التحقق من وضعية المجموعة كشرط.

1. قم بتكوين مستخدمي AD ليكونوا أعضاء في مجموعة معينة. استخدم اسما يضعه في أعلى التدرج الهرمي للمجموعات (ASA-VPN-Consultants). في AD-LDAP، يتم تعريف عضوية المجموعة بواسطة سمة وضع AD. من المهم أن تكون المجموعة في أعلى وضع/مجموعة على أول تطابق قواعد تطبيق حاليا يمكنك لأنه نظرا في القائمة، السلسلة. في الإصدار 7.3، يمكنك إجراء التصفية والتنفيذ على عدة مجموعات.
2. على ASA، قم بإنشاء خريطة سمة ldap باستخدام الحد الأدنى للتعيين:
```
ldap attribute-map LDAP-MAP
map-name memberOf Tunneling-Protocols
map-value memberOf cn=ASA-VPN-Consultants,cn=Users,dc=abcd,dc=com 4
5540-1#
```
ملاحظة: إضافة المزيد من السمات إلى الخريطة حسب الحاجة. توضح هذه الأمثلة الحد الأدنى للتحكم في هذه الوظيفة المحددة (السماح بالوصول أو رفضه استنادا إلى ldap؟يمكن السماح بعرض أو تعيين خريطة سمة ldap؟ما إذا (المجموعة وضعية إلى للمستخدم=joe_advisor، وهو جزء من AD، وهو وضع في AD group ASA-VPN-Consultants بالوصول فقط إذا كان المستخدم يستخدم IPsec (tunnel-protocol=4=IPSec). يمكن للمستخدم=joe_advisor، وهو جزء من AD، فشل الوصول إلى VPN أثناء أي عميل وصول عن بعد آخر (PPTP/L2TP، L2TP/IPSec، WebVPN/SVC، وما إلى ذلك). لا يمكن السماح للمستخدم=bill_the_hacker بالدخول نظرا لعدم وجود وضعية في AD لدى المستخدم.

فرض Active Directory ل "قواعد ساعات/وقت اليوم لتسجيل الدخول"

تصف حالة الاستخدام هذه كيفية إعداد قواعد الوقت من اليوم وتنفيذها على AD/LDAP.

فيما يلي الإجراء المتبع للقيام بذلك:

1. على خادم AD/LDAP:اختر المستخدم.انقر بزر الماوس الأيمن فوق **خصائص**.اختر علامة التبويب عام (على سبيل المثال، علامة التبويب عام).اختر سمة لتعيين استخدامها) على سبيل المثال، حقل Office، يتم استخدامه لفرض النطاق الزمني، حقل/سمة،

وأدخل اسم النطاق الزمني (على سبيل المثال، بوسطن). يتم تخزين تكوين Office على واجهة المستخدم الرسومية في سمة AD/LDAP physicalDeliveryOfficeName.

2. على ال ASA إنشاء جدول تعيين سمة LDAP.تعيين سمة AD/LDAP "physicalDeliveryOfficeName" لسمة ASA "access-hours".مثال:

```
B200-54(config-time-range)# show run ldap
ldap attribute-map TimeOfDay
map-name physicalDeliveryOfficeName Access-Hours
```

3. في ASA، أرطب خريطة سمة LDAP بإدخال AAA-server:

```
B200-54(config-time-range)# show runn aaa-server microsoft
aaa-server microsoft protocol ldap
aaa-server microsoft host audi-qa.frdevtestad.local
ldap-base-dn dc=frdevtestad,dc=local
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password hello
ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
ldap-attribute-map TimeOfDay
```

4. على ASA، قم بإنشاء كائن نطاق زمني يحتوي على قيمة الاسم التي تم تعيينها للمستخدم (قيمة Office في الخطوة 1):

```
B200-54(config-time-range)# show runn time-range
!
time-range Boston
periodic weekdays 8:00 to 17:00
!
```

5. إنشاء جلسة عمل الوصول عن بعد إلى VPN: يمكن أن تنجح الجلسة إذا كانت ضمن النطاق الزمني.يمكن أن يفشل الجلسة إن خارج المدى الزمني.

أستخدم تكوين خريطة LDAP لتعيين مستخدم في نهج مجموعة محدد واستخدام الأمر authorization-server-group، في حالة المصادقة المزدوجة

1. في هذا السيناريو، تم إستخدام مصادقة مزدوجة. أول خادم مصادقة يستخدم هو خادم LDAP. قم بتكوين خادم LDAP، وموزو المصادقة الثاني المستخدم هو خادم RADIUS. وكذلك خادم RADIUS. فيما يلي مثال:

```
ASA5585-S10-K9# show runn aaa-server
aaa-server test-ldap protocol ldap
aaa-server test-ldap (out) host 10.201.246.130
 ldap-base-dn cn=users, dc=htts-sec, dc=com
 ldap-login-password *****
 ldap-login-dn cn=Administrator, cn=Users, dc=htts-sec, dc=com
 server-type microsoft
 ldap-attribute-map Test-Safenet-MAP
aaa-server test-rad protocol radius
aaa-server test-rad (out) host 10.201.249.102
 key *****
```

تعريف خريطة سمة LDAP. فيما يلي مثال:

```
ASA5585-S10-K9# show runn ldap
ldap attribute-map Test-Safenet-MAP
map-name memberOf IETF-Radius-Class
map-value memberOf "CN=DHCP Users,CN=Users,DC=htts-sec,DC=com" Test-Policy-Safenet
```

قم بتعريف مجموعة النفق وربط خادم RADIUS و LDAP للمصادقة. فيما يلي مثال:

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
default-group-policy NoAccess
```

```
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

عرض نهج المجموعة الذي يتم إستخدامه في تكوين مجموعة النفق:

```
ASA5585-S10-K9# show runn group-policy
group-policy NoAccess internal
group-policy NoAccess attributes
wins-server none
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 0
default-domain none
group-policy Test-Policy-Safenet internal
group-policy Test-Policy-Safenet attributes
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 15
vpn-idle-timeout 30
vpn-tunnel-protocol ikev1 ssl-client ssl-clientless
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Safenet-Group-Policy-SplitAcl
default-domain none
```

باستخدام هذا التكوين، لم يتم وضع مستخدمي AnyConnect الذين تم تعيينهم بشكل صحيح باستخدام سمات LDAP في نهج المجموعة واختبار النهج-SafeEt. وبدلا من ذلك، كانت لا تزال موضوعة في نهج المجموعة الافتراضي، في هذه الحالة NoAccess.رأيت القصاصة من ال debugs (debug ldap 255) و syslogs في مستوى معلومة:

```
------------------------------------------------------------------------------

memberOf: value = CN=DHCP Users,CN=Users,DC=htts-sec,DC=com

[47]                          mapped to IETF-Radius-Class: value = Test-Policy-Safenet

[47]                          mapped to LDAP-Class: value = Test-Policy-Safenet

------------------------------------------------------------------------------

Syslogs :

%ASA-6-113004: AAA user authentication Successful : server = 10.201.246.130 : user =
test123

%ASA-6-113003: AAA group policy for user test123 is set to Test-Policy-Safenet

%ASA-6-113011: AAA retrieved user specific group policy (Test-Policy-Safenet) for user =
test123

%ASA-6-113009: AAA retrieved default group policy (NoAccess) for user = test123

%ASA-6-113013: AAA unable to complete the request Error : reason = Simultaneous logins
exceeded for user : user = test123

%ASA-6-716039: Group <DfltGrpPolicy> User <test123> IP <10.116.122.154> Authentication:
rejected, Session Type: WebVPN.
```

تظهر هذه syslogs فشل حيث تم منح المستخدم نهج مجموعة NoAccess الذي تم تعيين تسجيل الدخول المتزامن عليه إلى 0 على الرغم من أن syslogs تقول إنه استرجع نهج مجموعة خاص بالمستخدم.من أجل أن يتم تعيين المستخدم في نهج المجموعة، استنادا إلى خريطة LDAP، يجب أن يكون لديك هذا الأمر: **authorization-server-group test-ldap** (في هذه الحالة، **يكون test-ldap** هو اسم خادم LDAP). فيما يلي مثال:

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
```

```
 secondary-authentication-server-group test-ldap use-primary-username
authorization-server-group test-ldap
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

2. الآن، إذا قام خادم المصادقة الأول (RADIUS، في هذا المثال) بإرسال سمات خاصة بالمستخدم، على سبيل المثال، سمة فئة IEFT، في هذه الحالة، يمكن تعيين المستخدم إلى نهج المجموعة الذي تم إرساله بواسطة RADIUS. وعلى الرغم من أن الخادم RADIUS الثاني يحتوي على خريطة LDAP تم تكوينها وأن سمات LDAP الخاصة بالمستخدم تقوم بتعيين المستخدم إلى نهج مجموعة مختلف، يمكن فرض نهج المجموعة الذي تم إرساله بواسطة خادم المصادقة الأول. لكي يتم وضع المستخدم في نهج مجموعة الاستئناف إلى سمة خريطة LDAP، يجب تحديد هذا الأمر ضمن مجموعة النفق: **authorization-server-group test-ldap**.
3. إذا كان خادم المصادقة الأول هو SDI أو OTP، والذي لا يمكن أن يرمي بالسمة الخاصة بالمستخدم، فسيكون المستخدم واقع في نهج المجموعة الافتراضي لمجموعة النفق. في هذه الحالة، NoAccess على الرغم من أن تعيين LDAP صحيح. في هذه الحالة، تحتاج أيضا إلى الأمر **authorization-server-group test-ldap**، أسفل مجموعة النفق الخاصة بالمستخدم وضعه في نهج المجموعة الصحيح.
4. إذا كان كل الخادمين هما نفس الخادمين RADIUS أو LDAP، فلن تكون بحاجة إلى الأمر **authorization-server-group** حتى يعمل قفل نهج المجموعة.

التحقق من الصحة

```
ASA5585-S10-K9# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : test123                  Index        : 2
Assigned IP  : 10.34.63.1             Public IP    : 10.116.122.154
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : 3DES 3DES 3DES         Hashing      : SHA1 SHA1 SHA1
Bytes Tx     : 14042                  Bytes Rx     : 8872
Group Policy : Test-Policy-Safenet    Tunnel Group : Test_Safenet
Login Time   : 10:45:28 UTC Fri Sep 12 2014
Duration     : 0h:01m:12s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

تصحيح أخطاء حركة LDAP

يمكن إستخدام عمليات تصحيح الأخطاء هذه للمساعدة في عزل المشاكل المتعلقة بتكوين DAP:

- debug ldap 255
- تتبع dap ل debug
- تصحيح أخطاء مصادقة aaa (المصادقة والتفويض والمحاسبة)

تعذر على ASA مصادقة المستخدمين من خادم LDAP

في حالة عدم قدرة ASA على مصادقة المستخدمين من خدمة LDAP، فيما يلي بعض تصحيح الأخطاء:

```
ldap 255 output:[1555805] Session Start[1555805] New request Session, context
0xcd66c028, reqType = 1[1555805]
Fiber started[1555805] Creating LDAP context with uri=ldaps://172.30.74.70:636
[1555805] Connect to LDAP server:
ldaps://172.30.74.70:636, status = Successful[1555805] supportedLDAPVersion:
value = 3[1555805]
supportedLDAPVersion: value = 2[1555805] Binding as administrator[1555805]
Performing Simple
authentication for sysservices to 172.30.74.70[1555805] Simple authentication
for sysservices returned code (49)
Invalid credentials[1555805] Failed to bind as administrator returned code
(-1) Can't contact LDAP server[1555805]
Fiber exit Tx=222 bytes Rx=605 bytes, status=-2[1555805] Session End
```

من هذه الأخطاء، إما أن تنسى LDAP Login DN غير صحيح وأ أن كلمة المرور غير صحيحة لذلك دقق كل in order to حلل تالإصدار.

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).