ASA 8.0: تكوين مصادقة LDAP لمستخدمي WebVPN

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين جهاز الأمان القابل للتكيف (ASA) من Cisco لاستخدام خادم LDAP لمصادقة مستخدمي WebVPN. خادم LDAP في هذا المثال هو Microsoft Active Directory. يتم تنفيذ هذا التكوين باستخدام Adaptive Security Device Manager (ASDM) 6.0(2) على ASA الذي يشغل الإصدار 8.0(2) من البرنامج.

ملاحظة: في هذا المثال، تم تكوين مصادقة بروتوكول الوصول إلى الدليل خفيف الوزن (LDAP) لمستخدمي WebVPN، ولكن يمكن إستخدام هذا التكوين لجميع الأنواع الأخرى من عملاء الوصول عن بعد أيضا. ما عليك سوى تعيين مجموعة خوادم AAA إلى ملف تعريف الاتصال المطلوب (مجموعة النفق)، كما هو موضح.

المتطلبات الأساسية

يلزم تكوين شبكة VPN أساسية. في هذا المثال، يتم إستخدام WebVPN.

معلومات أساسية

في هذا المثال، يتحقق ASA من خادم LDAP للتحقق من هوية المستخدمين الذين يصادق عليهم. لا تعمل هذه العملية كعملية إضافة تقليدية لخدمة مصادقة طلب اتصال المستخدم البعيد (RADIUS) أو نظام تحكم الوصول إلى وحدة تحكم الوصول إلى المحطة الطرفية (TACACS+). توضح هذه الخطوات، على مستوى عال، كيفية إستخدام ASA لخادم LDAP للتحقق من مسوغات المستخدم.

1. يقوم المستخدم ببدء اتصال ب ASA.
2. تم تكوين ASA لمصادقة ذلك المستخدم باستخدام خادم Microsoft Active Directory (AD)/LDAP.

3. يتم ربط ASA بخادم LDAP باستخدام بيانات الاعتماد التي تم تكوينها على ASA (المسؤول في هذه الحالة)، ويبحث عن اسم المستخدم المتوفر. يحصل المستخدم **admin** أيضا على بيانات الاعتماد المناسبة لسرد المحتويات داخل Active Directory. راجع http://support.microsoft.com/?id=320528 للحصول على مزيد من المعلومات حول كيفية منح امتيازات استعلام LDAP.**ملاحظة:** يدير موفر طرف ثالث موقع Microsoft على الويب http://support.microsoft.com/?id=320528 . لا تتحمل Cisco المسؤولية عن محتواها.
4. إذا تم العثور على اسم المستخدم، يحاول ASA الربط بخادم LDAP باستخدام بيانات الاعتماد التي قدمها المستخدم عند تسجيل الدخول.
5. إذا نجح الربط الثاني، تنجح المصادقة ويقوم ASA بمعالجة سمات المستخدم.**ملاحظة:** في هذا المثال، لا يتم إستخدام السمات لأي شيء. ارجع إلى ASA/PIX: تخطيط عملاء VPN إلى سياسات مجموعة VPN من خلال مثال تكوين LDAP لترى مثالا على كيفية معالجة ASA لسمات LDAP.

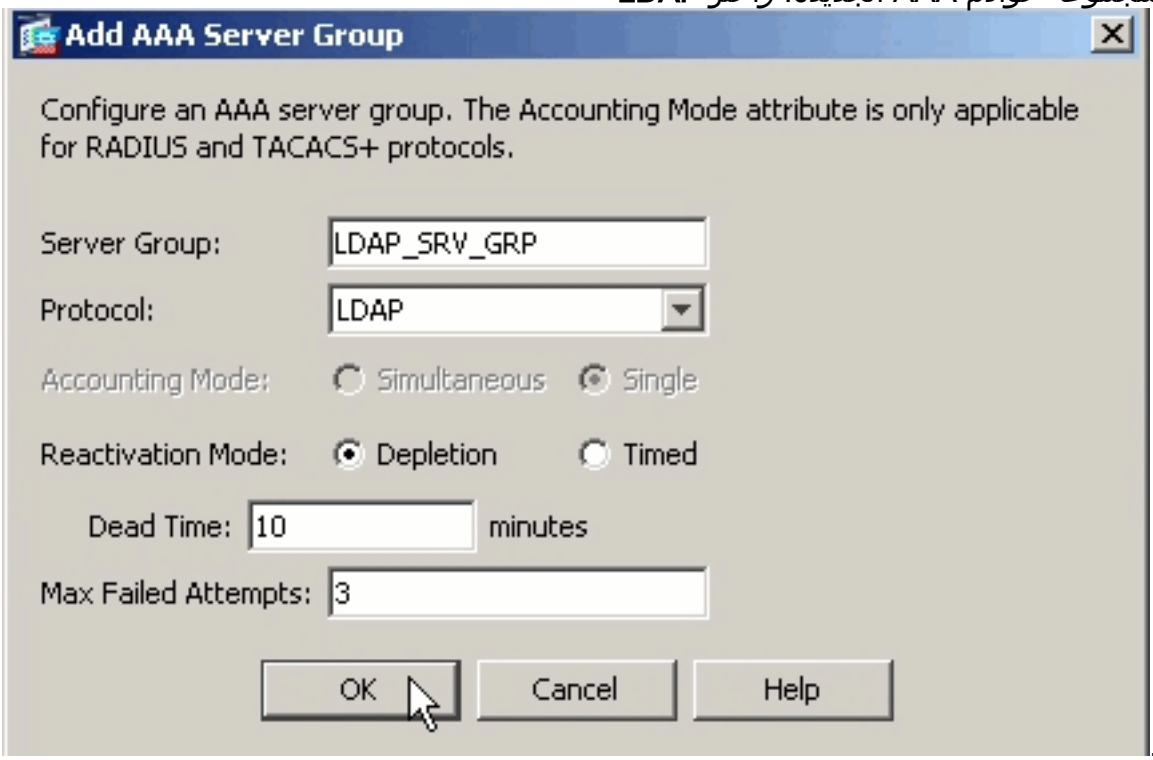
تكوين مصادقة LDAP

في هذا القسم، تقدم لك معلومات تكوين ASA لاستخدام خادم LDAP لمصادقة عملاء WebVPN.

ASDM

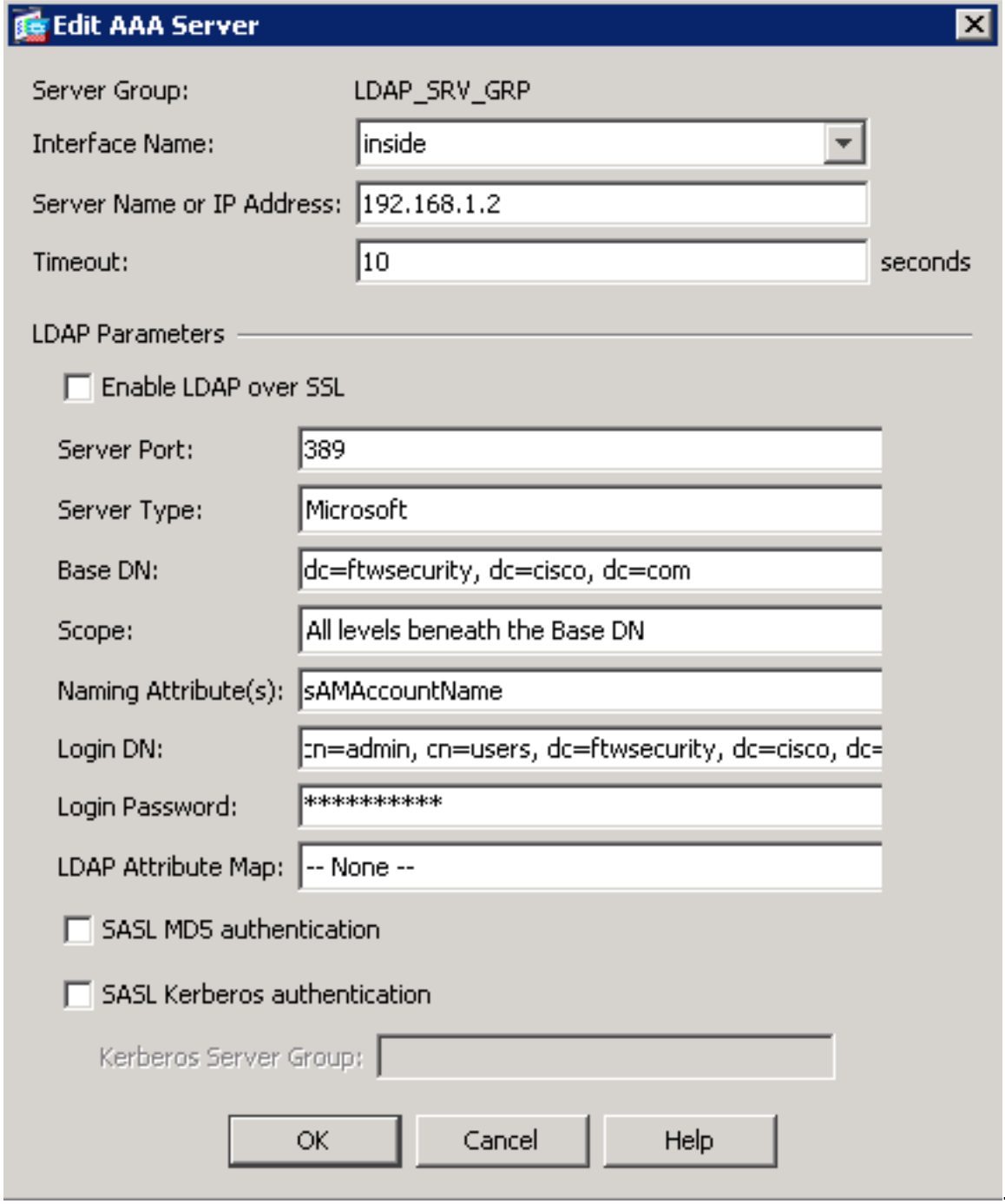
أتمت هذا steps في ال ASDM in order to شكلت ASA أن يتصل مع ال LDAP نادل ومصادقة WebVPN زبون.

1. انتقل إلى التكوين > Remote Access VPN (الوصول عن بعد) > إعداد AAA > مجموعات خوادم AAA.
2. انقر فوق **إضافة** بجوار مجموعات خوادم AAA
3. حدد اسم لمجموعة خوادم AAA الجديدة، واختر **LDAP** كبروتوكول.



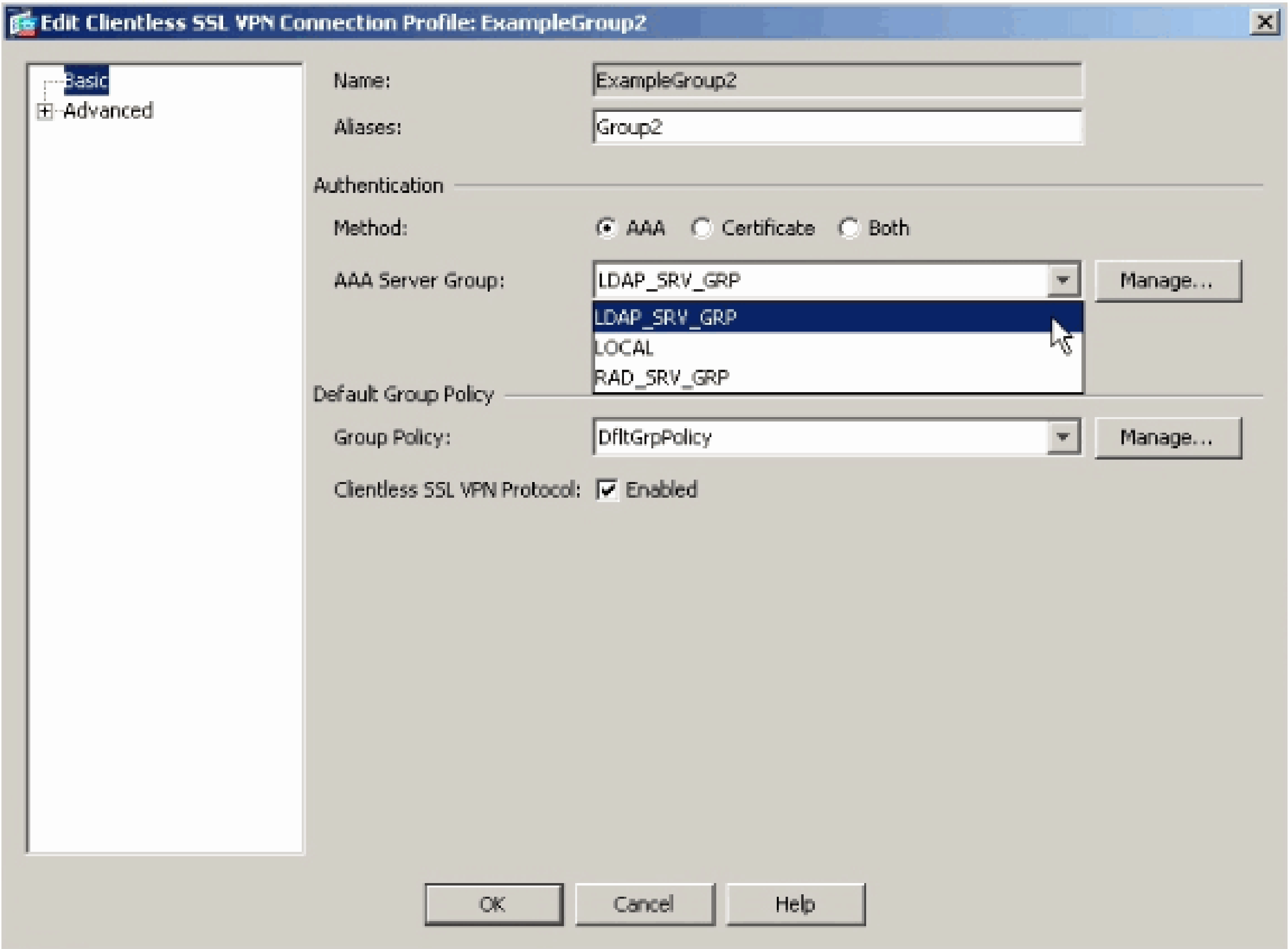
4. تأكد من تحديد مجموعتك الجديدة في الجزء العلوي، وانقر فوق **إضافة** بجوار **الخوادم في** جزء **المجموعة المحددة**.
5. توفير معلومات التكوين لخادم LDAP. توضح لقطة الشاشة التالية مثالا للتكوين. هذا شرح للعديد من خيارات التكوين:**اسم الواجهة**- الواجهة التي يستخدمها ASA للوصول إلى خادم LDAP**اسم الخادم أو عنوان IP**- العنوان الذي يستخدمه ASA للوصول إلى خادم LDAP**نوع الخادم**- نوع خادم LDAP، مثل MicrosoftDN **الأساسي**- الموقع في التدرج الهرمي LDAP حيث يجب أن يبدأ الخادم في البحث**النطاق**—مدى البحث في التدرج الهرمي ل LDAP الذي يجب أن يقوم به الخادم**سمة التسمية**- سمة الاسم المميز النسبي (أو السمات) التي

تعرف بشكل فريد إدخالا على خادم LDAP. **SAMAccountName** هي السمة الافتراضية في Microsoft Active Directory. السمات الأخرى الشائعة الاستخدام هي CN و UID و **DN**.userPrincipalName الخاص **بتسجيل الدخول**—DN مع امتيازات كافية لتمكين البحث/القراءة/البحث عن المستخدمين في خادم LDAP**كلمة مرور تسجيل الدخول**- كلمة المرور لحساب DN**مخطط سمة LDAP**- مخطط سمة LDAP المطلوب إستخدامه مع الاستجابات من هذا الخادم. ارجع إلى ASA/PIX: تعيين عملاء VPN إلى سياسات مجموعة VPN من خلال مثال تكوين LDAP للحصول على مزيد من المعلومات حول كيفية تكوين خرائط سمات



LDAP.

6. بمجرد تكوين مجموعة خوادم AAA وإضافة خادم إليها، من الضروري تكوين ملف تعريف الاتصال (مجموعة النفق) لاستخدام تكوين AAA الجديد. انتقل إلى التكوين > Remote Access VPN (الوصول عن بعد) > ClientLess SSL VPN Access > ملفات تعريف الاتصال.
7. أختر ملف تعريف الاتصال (مجموعة النفق) الذي تريد تكوين AAA له، وانقر فوق **تحرير**
8. تحت **المصادقة**، أختر مجموعة خوادم LDAP التي قمت بإنشائها سابقا.



واجهة سطر الأوامر

أتمت هذا steps في الأمر خط قارن (CLI) in order to شكلت ال ASA أن يتصل مع ال LDAP نادل ومصادقة WebVPN زبون.

```
ciscoasa#configure terminal

Configure the AAA Server group. ciscoasa(config)#aaa-server LDAP_SRV_GRP protocol ldap !--- ---!
    Configure the AAA Server. ciscoasa(config-aaa-server-group)#aaa-server LDAP_SRV_GRP (inside)
  host 192.168.1.2 ciscoasa(config-aaa-server-host)#ldap-base-dn dc=ftwsecurity, dc=cisco, dc=com
    ciscoasa(config-aaa-server-host)#ldap-login-dn cn=admin, cn=users, dc=ftwsecurity, dc=cisco,
     dc=com ciscoasa(config-aaa-server-host)#ldap-login-password ********** ciscoasa(config-aaa-
   server-host)#ldap-naming-attribute sAMAccountName ciscoasa(config-aaa-server-host)#ldap-scope
      subtree ciscoasa(config-aaa-server-host)#server-type microsoft ciscoasa(config-aaa-server-
   host)#exit !--- Configure the tunnel group to use the new AAA setup. ciscoasa(config)#tunnel-
     group ExampleGroup2 general-att ciscoasa(config-tunnel-general)#authentication-server-group
                                                                                    LDAP_SRV_GRP
```

إجراء عمليات بحث متعددة المجالات (إختياري)

اختياري. لا يساند ال ASA حاليا ال LDAP آلية حركية للبحث متعدد المجالات (cisco بق id CSCsj32153). يتم دعم عمليات البحث متعددة المجالات مع AD في وضع خادم الكتالوج العمومي. لإجراء عمليات بحث متعددة المجالات، قم بإعداد خادم AD لوضع خادم الكتالوج العمومي، عادة مع هذه المعلمات الأساسية لإدخال خادم LDAP في ASA. المفتاح هو إستخدام سمة ldap-name التي يجب أن تكون فريدة عبر شجرة الدليل.

```
server-port 3268
ldap-scope subtree
```

```
ldap-naming-attribute userPrincipalName
```

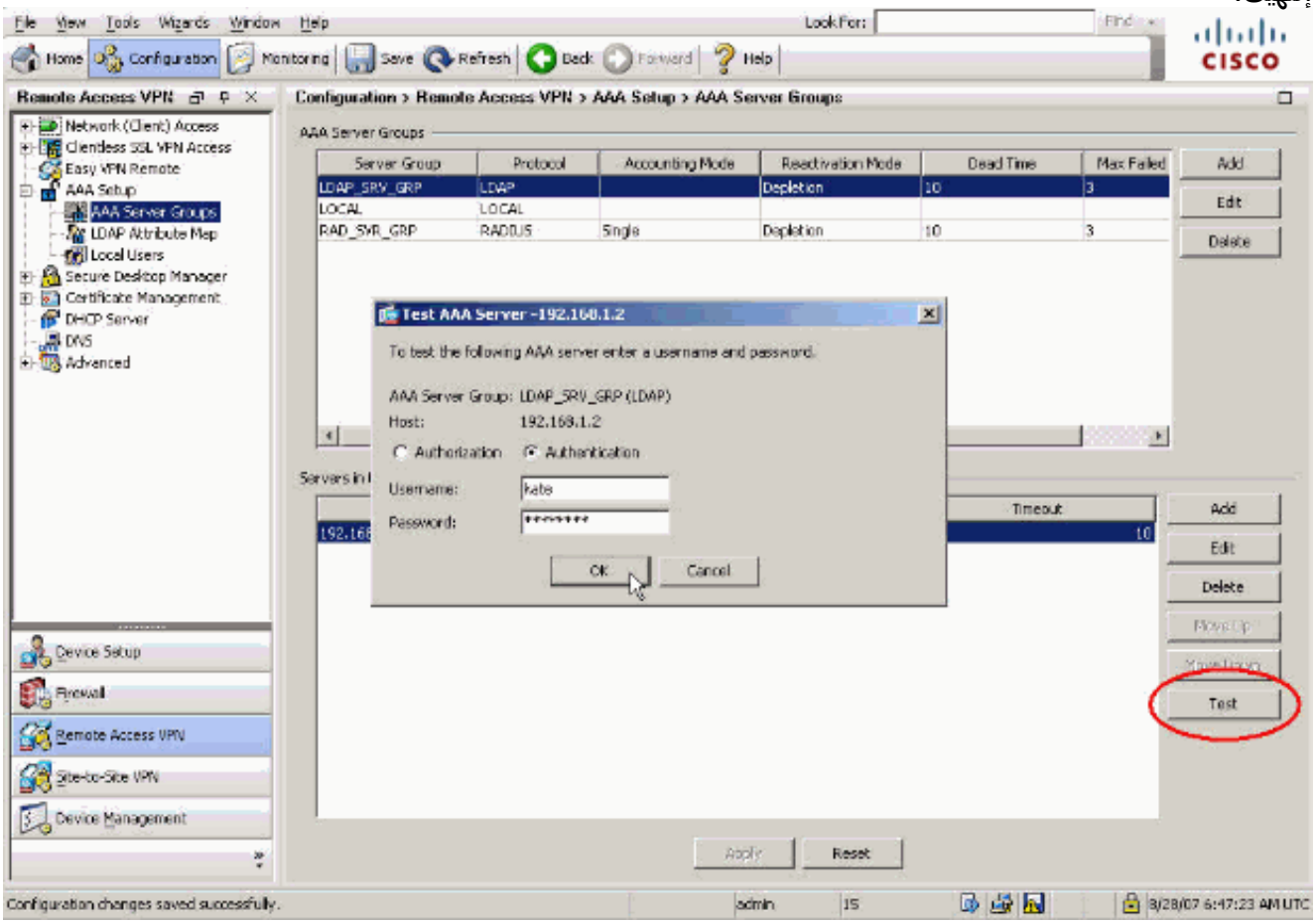
التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

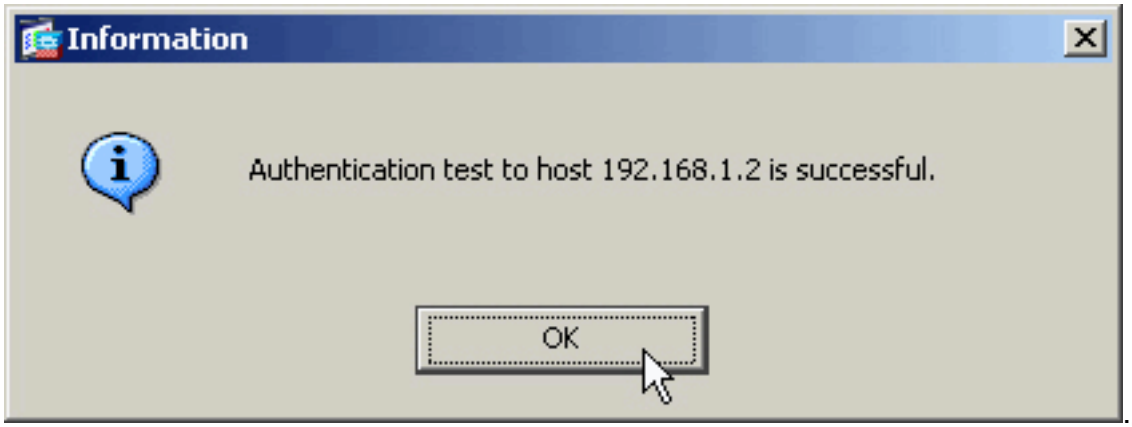
إختبار مع ASDM

تحقق من تكوين LDAP الخاص بك باستخدام الزر **Test** على شاشة تكوين مجموعات خوادم AAA. بمجرد توفير اسم مستخدم وكلمة مرور، يسمح لك هذا الزر بإرسال طلب مصادقة إختبار إلى خادم LDAP.

1. انتقل إلى التكوين > Remote Access VPN (الوصول عن بعد) > إعداد AAA > مجموعات خوادم AAA.
2. حدد مجموعة خوادم AAA المطلوبة في الجزء العلوي.
3. حدد خادم AAA الذي تريد إختباره في الجزء السفلي.
4. انقر فوق زر **إختبار** الموجود على يمين الجزء السفلي.
5. في الإطار الذي يظهر، انقر زر **مصادقة** الراديو، وقم بتوفير المسوغات التي تريد إختبارها. طقطقة **ok** عندما إنتهيت.



6. بعد أن يتصل ASA بخادم LDAP، تظهر رسالة نجاح أو



فشل.

إختبار مع CLI

يمكنك إستخدام الأمر **test** على سطر الأوامر لاختبار إعداد AAA الخاص بك. يتم إرسال طلب إختبار إلى خادم AAA، وتظهر النتيجة على سطر الأوامر.

```
ciscoasa#test aaa-server authentication LDAP_SRV_GRP host 192.168.1.2
                                    username kate password cisco123
<INFO: Attempting Authentication test to IP address <192.168.1.2
                                    (timeout: 12 seconds)
INFO: Authentication Successful
```

استكشاف الأخطاء وإصلاحها

إذا لم تكن متأكدا من سلسلة DN الحالية لاستخدامها، يمكنك إصدار الأمر **dsquery** على خادم التشغيل Windows Active من موجه أوامر للتحقق من سلسلة DN المناسبة لكائن مستخدم.

```
C:\Documents and Settings\Administrator>dsquery user -samid kate

Queries Active Directory for samid id "kate" "CN=Kate ---!
"Austen,CN=Users,DC=ftwsecurity,DC=cisco,DC=com
```

يمكن أن يساعد الأمر **debug ldap 255** في أستكشاف أخطاء المصادقة وإصلاحها في هذا السيناريو. يتيح هذا الأمر إمكانية تصحيح أخطاء LDAP ويسمح لك بمشاهدة العملية التي يستخدمها ASA للاتصال بخادم LDAP. تظهر هذه المخرجات اتصال ASA بخادم LDAP كما هو موضح في قسم معلومات الخلفية في هذا المستند.

يظهر تصحيح الأخطاء هذا مصادقة ناجحة:

```
ciscoasa#debug ldap 255
                                    Session Start [7]
                New request Session, context 0xd4b11730, reqType = 1 [7]
                                    Fiber started [7]
            Creating LDAP context with uri=ldap://192.168.1.2:389 [7]
Connect to LDAP server: ldap://192.168.1.2:389, status = Successful [7]
        defaultNamingContext: value = DC=ftwsecurity,DC=cisco,DC=com [7]
                                    supportedLDAPVersion: value = 3 [7]
                                    supportedLDAPVersion: value = 2 [7]
                        supportedSASLMechanisms: value = GSSAPI [7]
                    supportedSASLMechanisms: value = GSS-SPNEGO [7]
                      supportedSASLMechanisms: value = EXTERNAL [7]
                    supportedSASLMechanisms: value = DIGEST-MD5 [7]

The ASA connects to the LDAP server as admin to search for kate. [7] Binding as ---!
                                    administrator
```

```
                                Performing Simple authentication for admin to 192.168.1.2 [7]
                                                                    :LDAP Search [7]
                                                [Base DN = [dc=ftwsecurity, dc=cisco, dc=com
                                                    [Filter  = [sAMAccountName=kate
                                                        [Scope   = [SUBTREE
                            [User DN = [CN=Kate Austen,CN=Users,DC=ftwsecurity,DC=cisco,DC=com [7]
                                                Talking to Active Directory server 192.168.1.2 [7]
                                    ,Reading password policy for kate, dn:CN=Kate Austen,CN=Users [7]
                                                                    DC=ftwsecurity,DC=cisco,DC=com
                                                            Read bad password count 1 [7]

The ASA binds to the LDAP server as kate to test the password. [7] Binding as user ---!
                                Performing Simple authentication for kate to 192.168.1.2 [7]
                                                    Checking password policy for user kate [7]
                                                                Binding as administrator [7]
                                Performing Simple authentication for admin to 192.168.1.2 [7]
                                        Authentication successful for kate to 192.168.1.2 [7]
                                    Retrieving user attributes from server 192.168.1.2 [7]
                                                                    :Retrieved Attributes [7]
                                                            objectClass: value = top     [7]
                                                         objectClass: value = person     [7]
                                                 objectClass: value = organizationalPerson     [7]
                                                            objectClass: value = user     [7]
                                                              cn: value = Kate Austen     [7]
                                                                   sn: value = Austen     [7]
                                                             givenName: value = Kate     [7]
                        ,distinguishedName: value = CN=Kate Austen,CN=Users,DC=ftwsecurity     [7]
                                                                    DC=cisco,DC=com
                                                             instanceType: value = 4     [7]
                                                    whenCreated: value = 20070815155224.0Z     [7]
                                                    whenChanged: value = 20070815195813.0Z     [7]
                                                          displayName: value = Kate Austen     [7]
                                                                uSNCreated: value = 16430     [7]
                    memberOf: value = CN=Castaways,CN=Users,DC=ftwsecurity,DC=cisco,DC=com     [7]
                    memberOf: value = CN=Employees,CN=Users,DC=ftwsecurity,DC=cisco,DC=com     [7]
                                                             uSNChanged: value = 20500     [7]
                                                             name: value = Kate Austen     [7]
                                                .....objectGUID: value = ..z...yC.q0     [7]
                                                   userAccountControl: value = 66048     [7]
                                                              badPwdCount: value = 1     [7]
                                                                 codePage: value = 0     [7]
                                                             countryCode: value = 0     [7]
                                                badPasswordTime: value = 128321799570937500     [7]
                                                                 lastLogoff: value = 0     [7]
                                                lastLogon: value = 128321798130468750     [7]
                                                pwdLastSet: value = 128316667442656250     [7]
                                                          primaryGroupID: value = 513     [7]
                                        ...objectSid: value = ............Q..p..*.p?E.Z     [7]
                                            accountExpires: value = 9223372036854775807     [7]
                                                             logonCount: value = 0     [7]
                                                    sAMAccountName: value = kate     [7]
                                                sAMAccountType: value = 805306368     [7]
                                    userPrincipalName: value = kate@ftwsecurity.cisco.com     [7]
                        ,objectCategory: value = CN=Person,CN=Schema,CN=Configuration     [7]
                                                            DC=ftwsecurity,DC=cisco,DC=com
                                    dSCorePropagationData: value = 20070815195237.0Z     [7]
                                    dSCorePropagationData: value = 20070815195237.0Z     [7]
                                    dSCorePropagationData: value = 20070815195237.0Z     [7]
                                    dSCorePropagationData: value = 16010108151056.0Z     [7]
                                        Fiber exit Tx=685 bytes Rx=2690 bytes, status=1 [7]
                                                                            Session End [7]
```

يوضح تصحيح الأخطاء هذا المصادقة التي تفشل بسبب كلمة مرور غير صحيحة:

```
ciscoasa#debug ldap 255
Session Start [8]
New request Session, context 0xd4b11730, reqType = 1 [8]
Fiber started [8]
Creating LDAP context with uri=ldap://192.168.1.2:389 [8]
Connect to LDAP server: ldap://192.168.1.2:389, status = Successful [8]
defaultNamingContext: value = DC=ftwsecurity,DC=cisco,DC=com [8]
supportedLDAPVersion: value = 3 [8]
supportedLDAPVersion: value = 2 [8]
supportedSASLMechanisms: value = GSSAPI [8]
supportedSASLMechanisms: value = GSS-SPNEGO [8]
supportedSASLMechanisms: value = EXTERNAL [8]
supportedSASLMechanisms: value = DIGEST-MD5 [8]

The ASA connects to the LDAP server as admin to search for kate. [8] Binding as ---!
administrator
Performing Simple authentication for admin to 192.168.1.2 [8]
:LDAP Search [8]
[Base DN = [dc=ftwsecurity, dc=cisco, dc=com
[Filter = [sAMAccountName=kate
[Scope = [SUBTREE
[User DN = [CN=Kate Austen,CN=Users,DC=ftwsecurity,DC=cisco,DC=com [8]
Talking to Active Directory server 192.168.1.2 [8]
,Reading password policy for kate, dn:CN=Kate Austen,CN=Users [8]
DC=ftwsecurity,DC=cisco,DC=com
Read bad password count 1 [8]

The ASA attempts to bind as kate, but the password is incorrect. [8] Binding as user ---!
Performing Simple authentication for kate to 192.168.1.2 [8]
Simple authentication for kate returned code (49) Invalid credentials [8]
Binding as administrator [8]
Performing Simple authentication for admin to 192.168.1.2 [8]
,Reading bad password count for kate, dn: CN=Kate Austen,CN=Users [8]
DC=ftwsecurity,DC=cisco,DC=com
Received badPwdCount=1 for user kate [8]
badPwdCount=1 before, badPwdCount=1 after for kate [8]
,now: Tue, 28 Aug 2007 15:33:05 GMT, lastset: Wed, 15 Aug 2007 15:52:24 GMT [8]
delta=1122041, maxage=3710851 secs
Invalid password for kate [8]
Fiber exit Tx=788 bytes Rx=2904 bytes, status=-1 [8]
Session End [8]
```

يعرض تصحيح الأخطاء هذا مصادقة تفشل بسبب تعذر العثور على المستخدم على خادم LDAP:

```
ciscoasa#debug ldap 255
Session Start [9]
New request Session, context 0xd4b11730, reqType = 1 [9]
Fiber started [9]
Creating LDAP context with uri=ldap://192.168.1.2:389 [9]
Connect to LDAP server: ldap://192.168.1.2:389, status = Successful [9]
defaultNamingContext: value = DC=ftwsecurity,DC=cisco,DC=com [9]
supportedLDAPVersion: value = 3 [9]
supportedLDAPVersion: value = 2 [9]
supportedSASLMechanisms: value = GSSAPI [9]
supportedSASLMechanisms: value = GSS-SPNEGO [9]
supportedSASLMechanisms: value = EXTERNAL [9]
supportedSASLMechanisms: value = DIGEST-MD5 [9]

The user mikhail is not found. [9] Binding as administrator ---!
Performing Simple authentication for admin to 192.168.1.2 [9]
:LDAP Search [9]
[Base DN = [dc=ftwsecurity, dc=cisco, dc=com
```

```
[Filter  = [sAMAccountName=mikhail
[Scope   = [SUBTREE
Requested attributes not found [9]
Fiber exit Tx=256 bytes Rx=607 bytes, status=-1 [9]
Session End [9]
```

تظهر الأخطاء رسالة الخطأ هذه عندما لا يعمل الاتصال بين ASA وخادم مصادقة LDAP:

```
ciscoasa# debug webvpn 255
.INFO: debug webvpn  enabled at level 255
[ciscoasa# webvpn_portal.c:ewaFormSubmit_webvpn_login[2162
ewaFormSubmit_webvpn_login: tgCookie = NULL
ewaFormSubmit_webvpn_login: cookie = 1
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
[not resuming [2587....
[webvpn_portal.c:http_webvpn_kill_cookie[787
[webvpn_auth.c:http_webvpn_pre_authentication[2327
!(WebVPN: calling AAA with ewsContext (-847917520) and nh (-851696992
[webvpn_auth.c:webvpn_add_auth_handle[5118
...WebVPN: started user authentication
[webvpn_auth.c:webvpn_aaa_callback[5158
(WebVPN: AAA status = (ERROR
[webvpn_portal.c:ewaFormSubmit_webvpn_login[2162
ewaFormSubmit_webvpn_login: tgCookie = NULL
ewaFormSubmit_webvpn_login: cookie = 1
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
[resuming [2564....
[webvpn_auth.c:http_webvpn_post_authentication[1506
.WebVPN: user: (utrcd01) auth error
```

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

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).