ACS 5.x: مثال تكوين خادم LDAP الآمن

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
معلومات أساسية
التكوين
تثبيت شهادة المرجع المصدق الجذر على ACS 5.x
تكوين ACS 5.x لبروتوكول LDAP الآمن
تكوين مخزن الهوية
استكشاف الأخطاء واصلاحها
معلومات ذات صلة

المقدمة

البروتوكول الخفيف للوصول للدليل (LDAP) هو بروتوكول شبكة للاستعلام عن خدمات الدليل التي تعمل على TCP/IP و UDP وتعديلها. LDAP هي آلية خفيفة الوزن للوصول إلى خادم دليل مستند إلى x.500. يحدد RFC 2251 بروتوكول LDAP.

يتم دمج Access Control Server (ACS) 5.x مع قاعدة بيانات LDAP خارجية، والتي تسمى أيضا مخزن هوية، باستخدام بروتوكول LDAP. هناك طريقتان للاتصال بخادم LDAP: اتصال نص عادي (بسيط) واتصال SSL (مشفر). يمكن تكوين ACS 5.x للاتصال بخادم LDAP باستخدام الطريقتين. في هذا المستند، يتم تكوين ACS 5.x للاتصال بخادم LDAP باستخدام اتصال مشفر.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن ACS 5.x لديه اتصال IP بخادم LDAP ومنفذ TCP 636 مفتوح.

يلزم تكوين خادم Microsoft® Active Directory LDAP لقبول إتصالات LDAP الآمنة على منفذ TCP 636. يفترض هذا المستند أن لديك الشهادة الجذر الخاصة بالمرجع المصدق (CA) الذي قام بإصدار شهادة الخادم إلى خادم Microsoft LDAP. لمزيد من المعلومات حول كيفية تكوين خادم LDAP، ارجع إلى كيفية تمكين LDAP عبر SSL باستخدام مرجع مصدق من جهة خارجية.

المكونات المستخدمة

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

- Cisco Secure ACS 5.x
- خادم LDAP ل Microsoft Active Directory

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.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

خدمة Directory

خدمة الدليل هي تطبيق برمجي، أو مجموعة تطبيقات، لتخزين وتنظيم المعلومات عن مستخدمي شبكة الكمبيوتر وموارد الشبكة. يمكنك إستخدام خدمة الدليل لإدارة وصول المستخدم إلى هذه الموارد.

تستند خدمة دليل LDAP إلى طراز عميل-خادم. يبدأ العميل جلسة LDAP بالاتصال بخادم LDAP، ويرسل طلبات العملية إلى الخادم. ثم يرسل الخادم استجاباته. يحتوي خادم LDAP واحد أو أكثر على بيانات من شجرة دليل LDAP أو قاعدة بيانات LDAP الخلفية.

تقوم خدمة الدليل بإدارة الدليل، وهو قاعدة البيانات التي تحتوي على المعلومات. تستخدم خدمات الدليل نموذج موزع لتخزين المعلومات، ويتم نسخ هذه المعلومات عادة بين خوادم الدليل.

يتم تنظيم دليل LDAP في تسلسل هرمي شجري بسيط ويمكن توزيعه على العديد من الخوادم. يمكن أن يحتوي كل خادم على إصدار منسوخ نسخا متماثلا من الدليل الإجمالي الذي تتم مزامنته بشكل دوري.

يحتوي مدخل الشجرة على مجموعة من السمات، حيث يكون لكل سمة اسم (نوع سمة أو وصف سمة) وقيمة أو أكثر. يتم تعريف السمات في مخطط.

يحتوي كل إدخال على معرف فريد: اسمه المميز (DN). يحتوي هذا الاسم على الاسم المميز النسبي (RDN) الذي تم إنشاؤه من السمات في الإدخال، متبوعا ب DN الخاص بالإدخال الأصل. يمكنك التفكير في DN كاسم ملف كامل، و RDN كاسم ملف نسبي في مجلد.

المصادقة باستخدام LDAP

يمكن ل ACS 5.x مصادقة أساسي مقابل مخزن تعريف LDAP عن طريق تنفيذ عملية ربط على خادم الدليل للعثور على الأساسي ومصادقته. وفي حالة نجاح المصادقة، يمكن ل ACS إسترداد المجموعات والسمات التي تنتمي إلى الأساسي. يمكن تكوين السمات المطلوب إستردادها في واجهة ويب ACS (صفحات LDAP). يمكن إستخدام هذه المجموعات والسمات من قبل ACS لتخويل الأساسي.

لمصادقة مستخدم أو الاستعلام عن مخزن تعريف LDAP، يتصل ACS بخادم LDAP ويحافظ على تجمع اتصال.

إدارة اتصال LDAP

يدعم ACS 5.x إتصالات LDAP المتزامنة المتعددة. يتم فتح الاتصالات عند الطلب في وقت مصادقة LDAP الأولى. تم تكوين الحد الأقصى لعدد الاتصالات لكل خادم LDAP. يؤدي فتح الاتصالات مقدما إلى تقليص وقت المصادقة.

يمكنك تعيين الحد الأقصى لعدد الاتصالات لاستخدامها لاتصالات الربط المتزامنة. يمكن أن يختلف عدد الاتصالات المفتوحة لكل خادم LDAP (أساسي أو ثانوي) ويتم تحديدها وفقا للحد الأقصى لعدد إتصالات الإدارة التي تم تكوينها لكل خادم.

يحتفظ ACS بقائمة من إتصالات LDAP المفتوحة (بما في ذلك معلومات الربط) لكل خادم LDAP تم تكوينه في ACS. أثناء عملية المصادقة، يحاول مدير الاتصال العثور على اتصال مفتوح من التجمع.

في حالة عدم وجود اتصال مفتوح، يتم فتح اتصال جديد. إذا قام خادم LDAP بإغلاق الاتصال، فتقوم إدارة الاتصال بالإعلام عن وجود خطأ أثناء الاتصال الأول للبحث في الدليل، وتحاول تجديد الاتصال.

بعد اكتمال عملية المصادقة، تطلق إدارة الاتصال الاتصال الاتصال بمدير الاتصال. أحلت ل كثير معلومة، ACS 5.x مستعمل مرشد.

التكوين

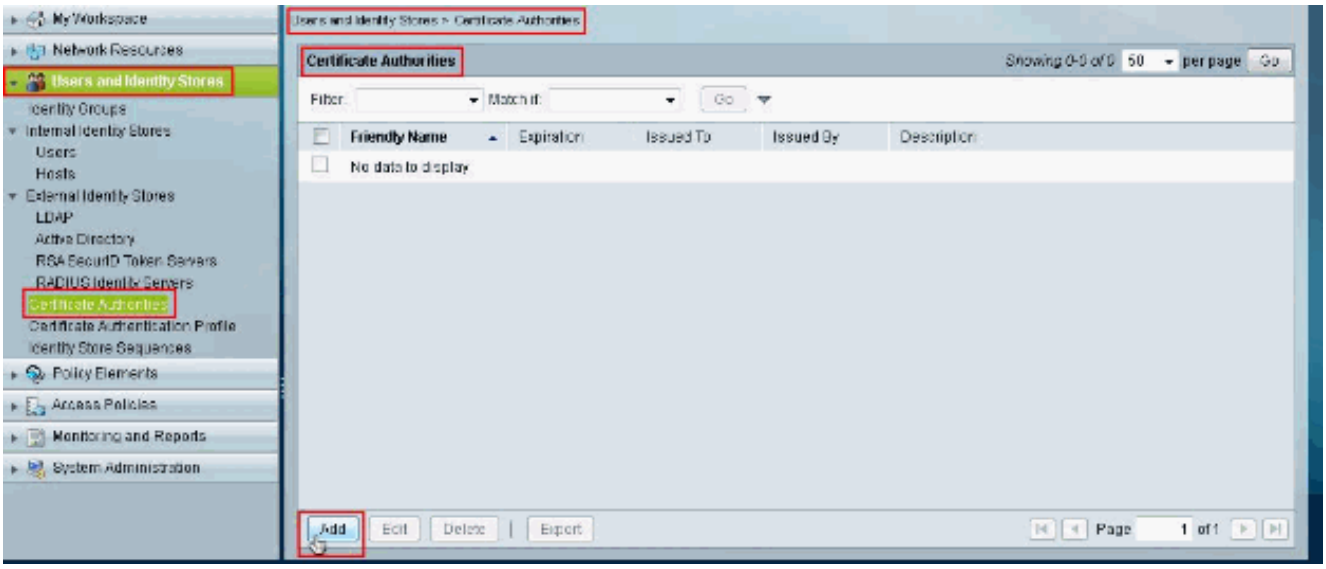
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

تثبيت شهادة المرجع المصدق الجذر على ACS 5.x

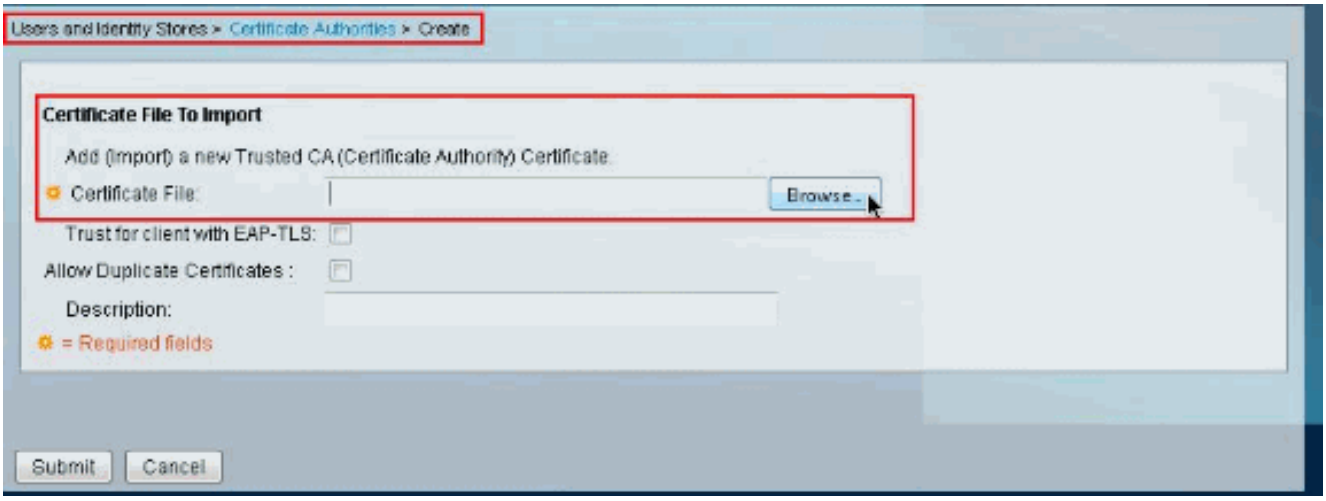
أتمت هذا steps in order to ركبت جذر ca شهادة على cisco يأمن acs 5.x:

ملاحظة: تأكد من تكوين خادم LDAP مسبقا لقبول الاتصالات المشفرة على منفذ TCP 636. لمزيد من المعلومات حول كيفية تكوين خادم Microsoft LDAP، ارجع إلى كيفية تمكين LDAP عبر SSL باستخدام مرجع مصدق من جهة خارجية.

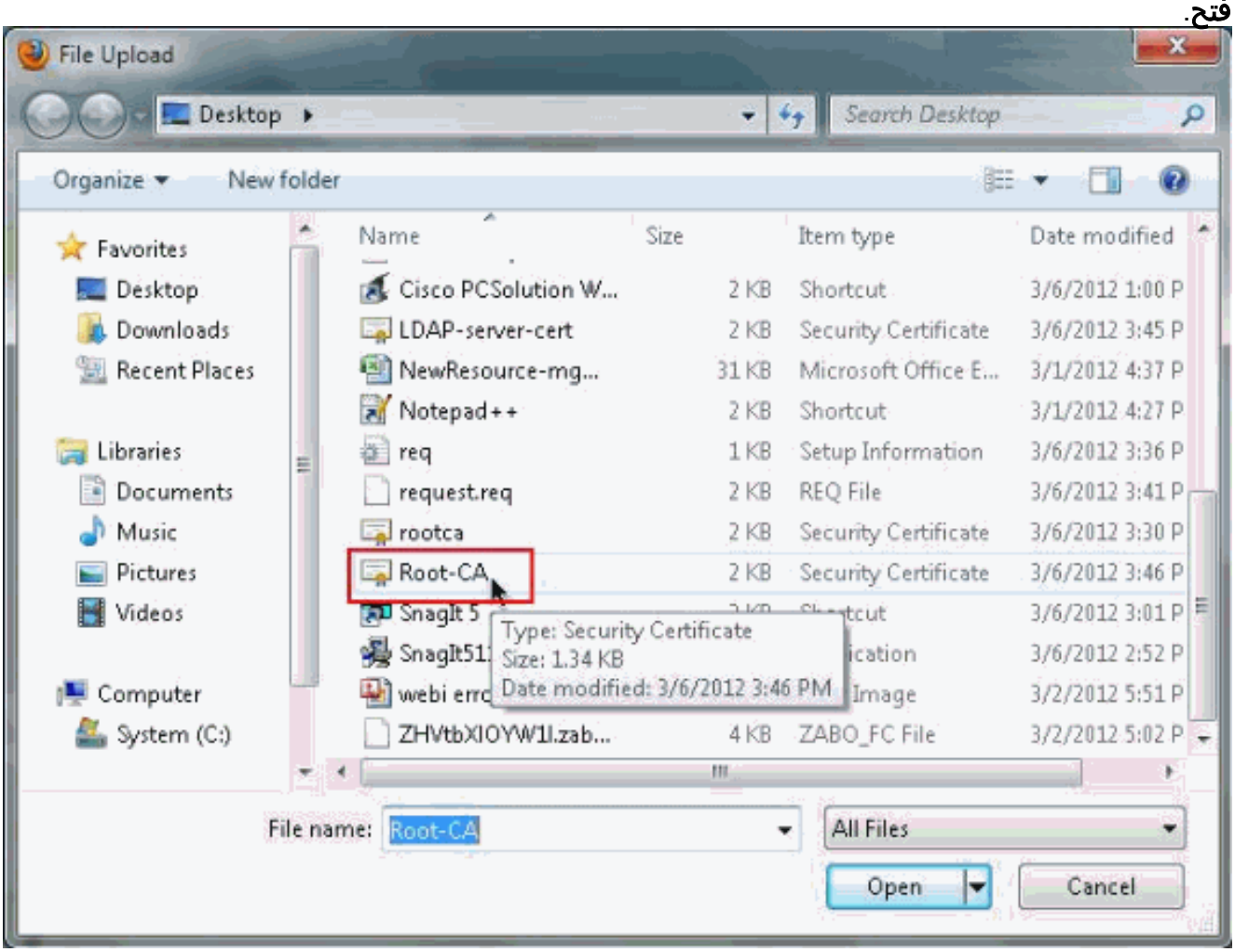
1. أختر **Users and Identity Store > Certificate Authority**، ثم انقر فوق **Add**لإضافة الشهادة الجذر الخاصة ب CA الذي أصدر شهادة الخادم إلى خادم Microsoft LDAP.



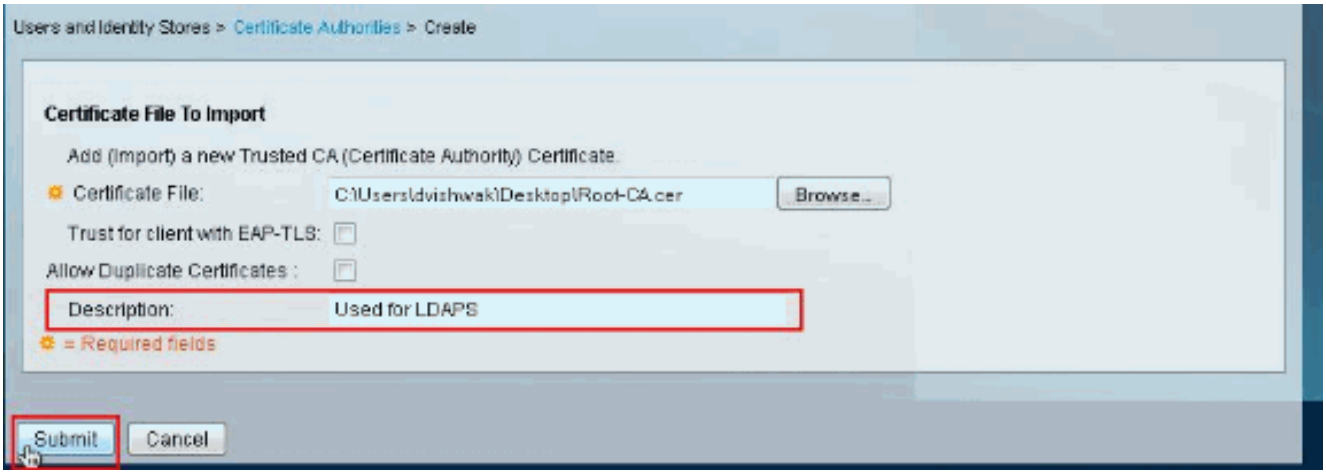
2. من قسم **ملف الترخيص إلى الاستيراد**، انقر **تصفح** بجوار **ملف الشهادة** للبحث عن ملف الترخيص.



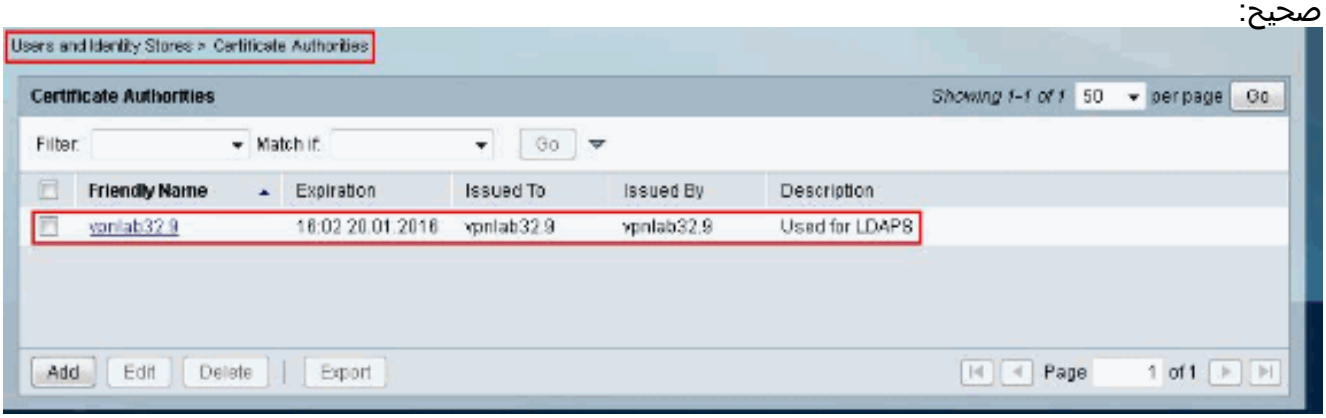
3. أختر **ملف الشهادة** المطلوب (الشهادة الجذر الخاصة ب CA الذي قام بإصدار شهادة الخادم إلى خادم Microsoft LDAP) وانقر على **فتح**.



4. توفير **وصف** في المساحة المتوفرة بجوار الوصف وانقر فوق **إرسال**.



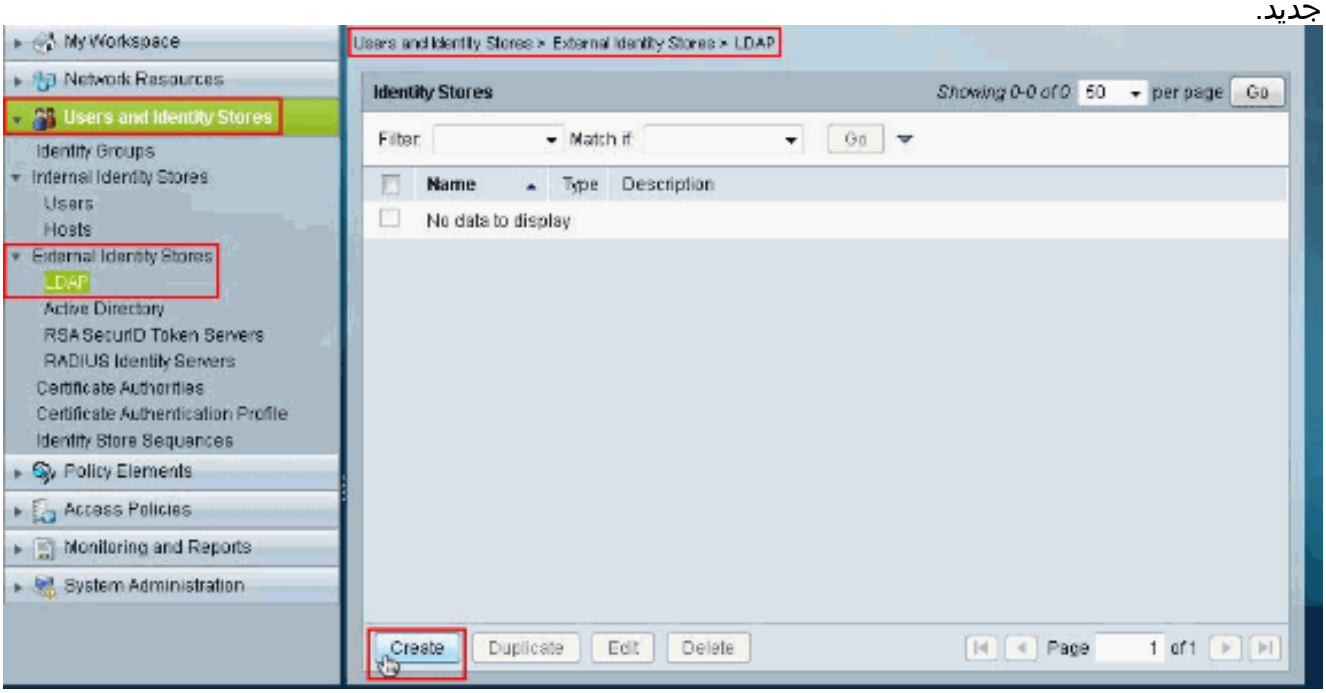
توضح هذه الصورة أن الشهادة الجذر قد تم تثبيتها بشكل صحيح:



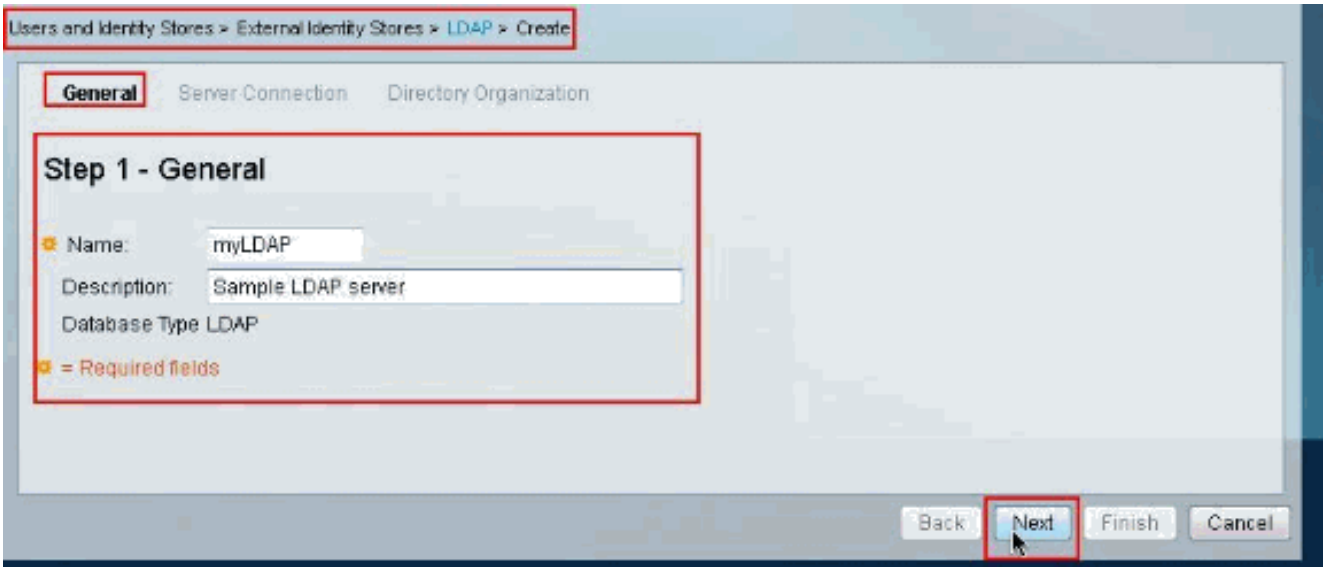
تكوين ACS 5.x لبروتوكول LDAP الآمن

أتمت هذا steps in order to شكلت ACS 5.x ل يأمن LDAP:

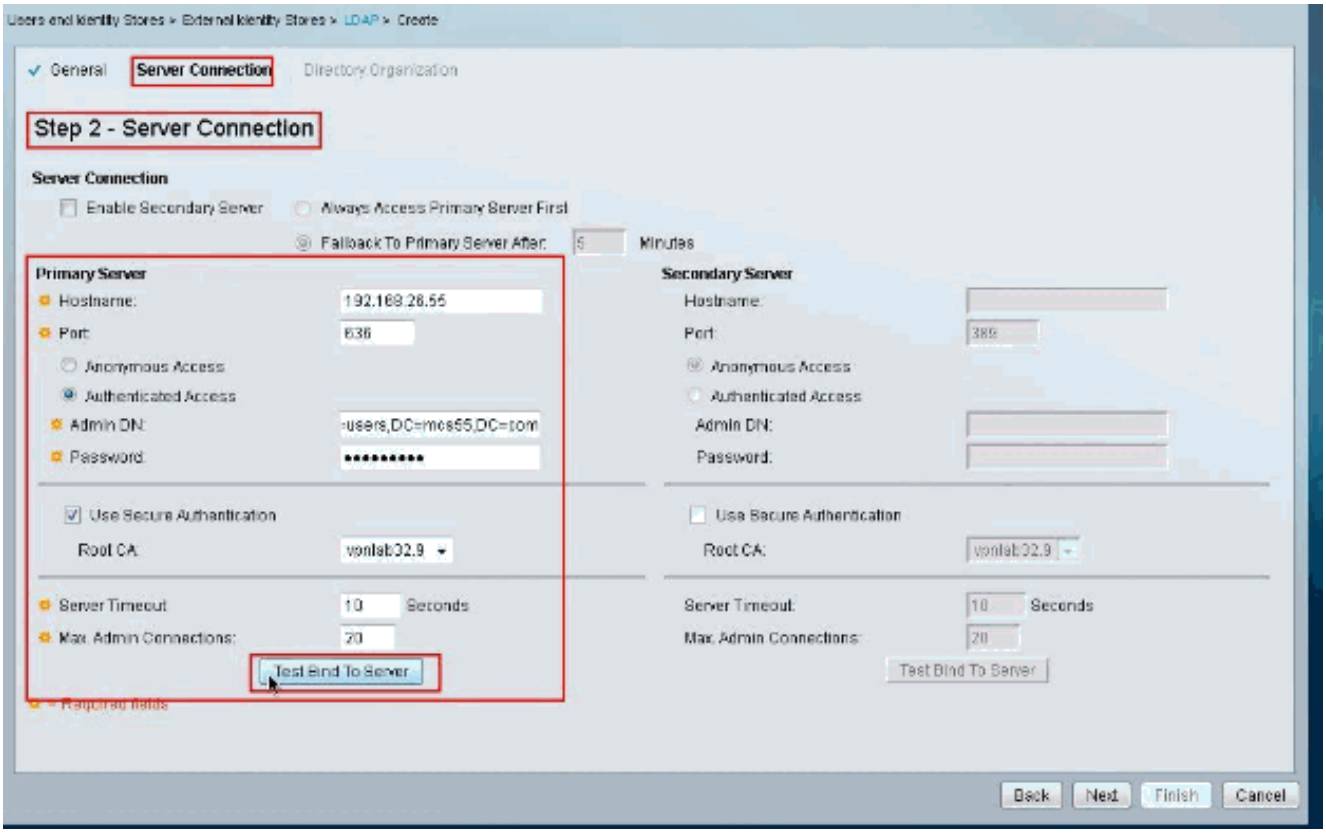
1. أختر **المستخدمين ومخازن الهوية > مخازن الهوية الخارجية > LDAP** وانقر **إنشاء** لإنشاء اتصال LDAP جديد.



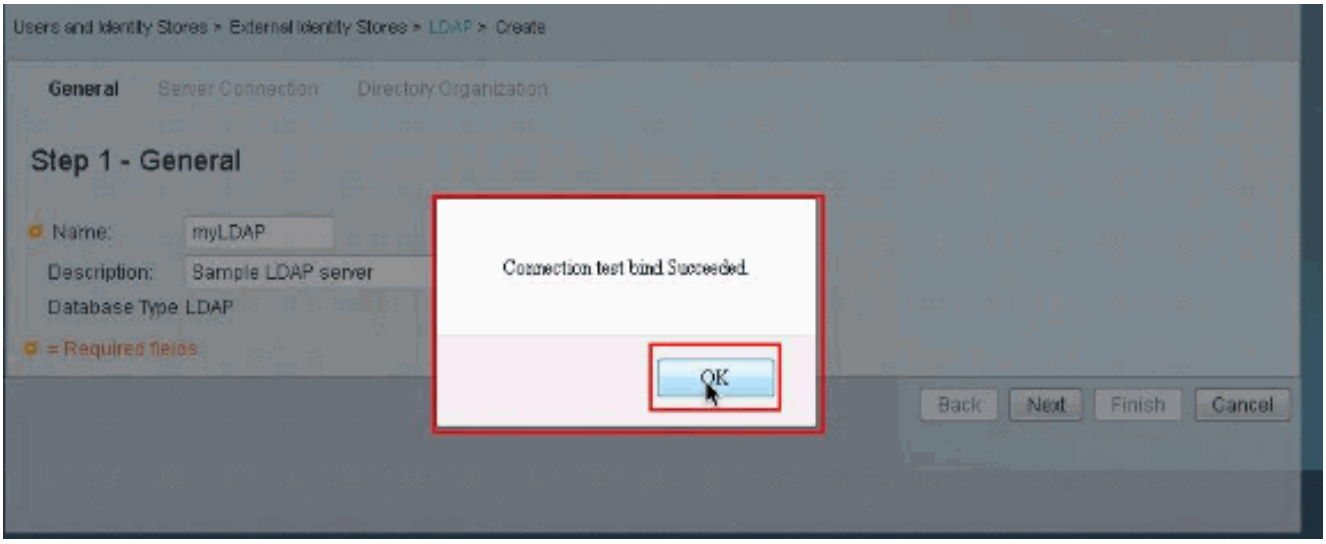
2. من علامة التبويب **عام**، قم بتوفير **الاسم** و**الوصف**(إختياري) ل LDAP الجديد، ثم انقر فوق **التالي**.



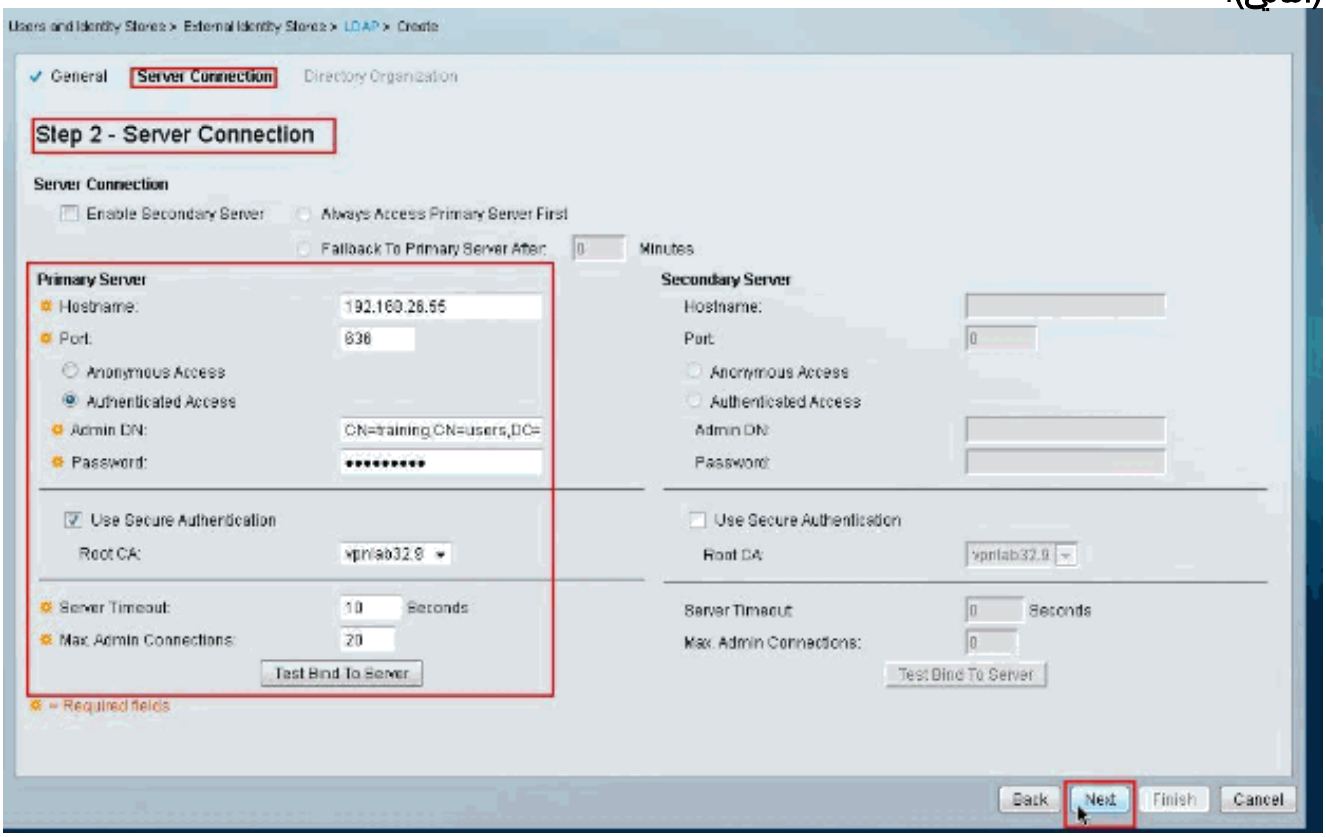
3. من علامة التبويب **اتصال الخادم** ضمن قسم **الخادم الأساسي**، قم بتوفير **hostname** و **port** و **admin DN** و **كلمة المرور**. تأكد من أن خانة الاختيار المجاورة **لاستخدام المصادقة الآمنة** محددة واختر **شهادة المرجع المصدق (CA) التي تم تثبيتها مؤخرا**. انقر فوق **إختبار الربط بالخادم**.**ملاحظة:** رقم المنفذ المعين من قبل IANA لبروتوكول LDAP الآمن هو 636 TCP. ومع ذلك، قم بتأكيد رقم المنفذ الذي يستخدمه خادم LDAP من مسؤول LDAP.**ملاحظة:** يجب أن يتم توفير DN للمسؤول وكلمة المرور لك بواسطة مسؤول LDAP الخاص بك. يجب أن يكون لدى Admin DN كافة الأذونات على كافة وحدات التحكم على خادم LDAP.



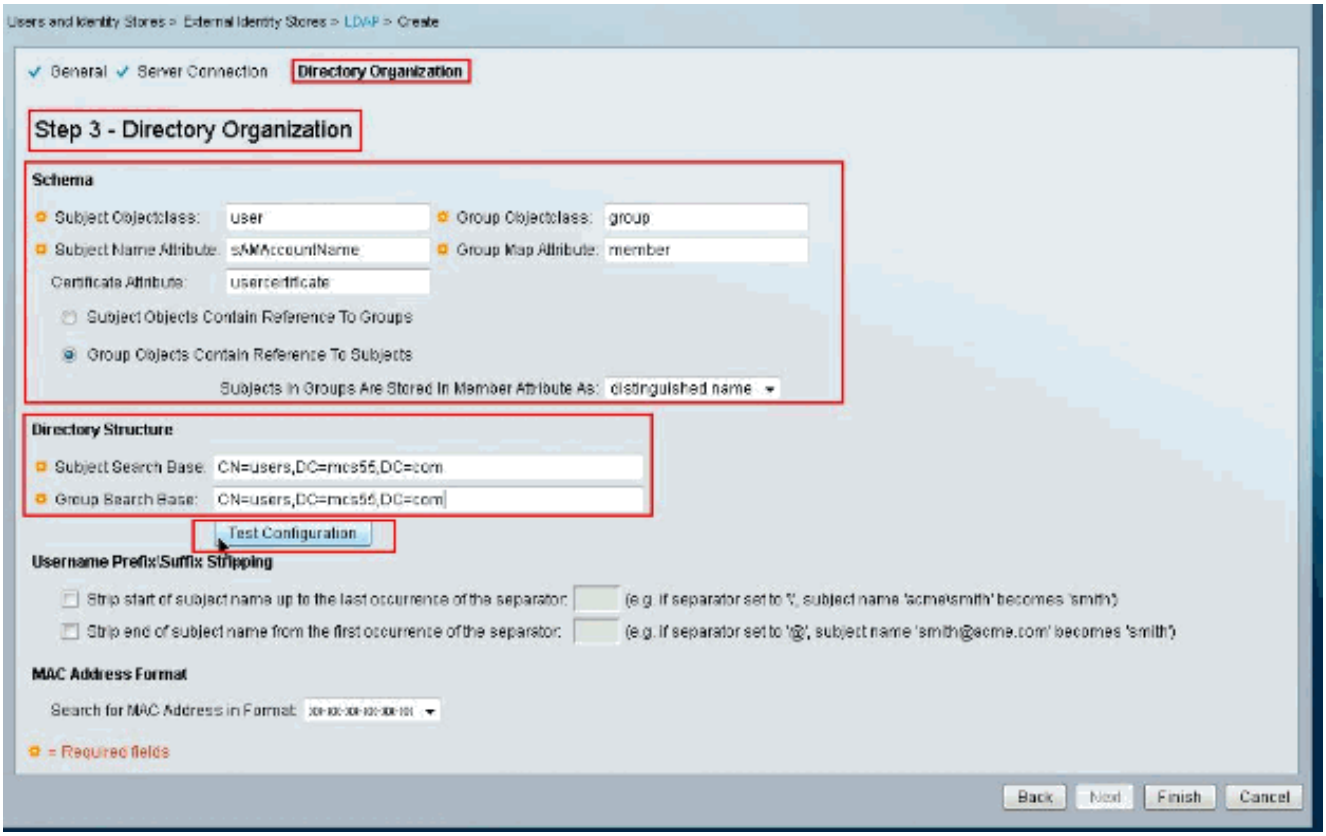
توضح الصورة التالية أن **ربط إختبار الاتصال بالخادم** تم بنجاح.**ملاحظة:** إذا لم ينجح إختبار الربط، فأعد التحقق من **اسم المضيف ورقم المنفذ وشبكة Admin DN وكلمة المرور** وكلمة المرور **الجذر** من مسؤول LDAP الخاص بك.



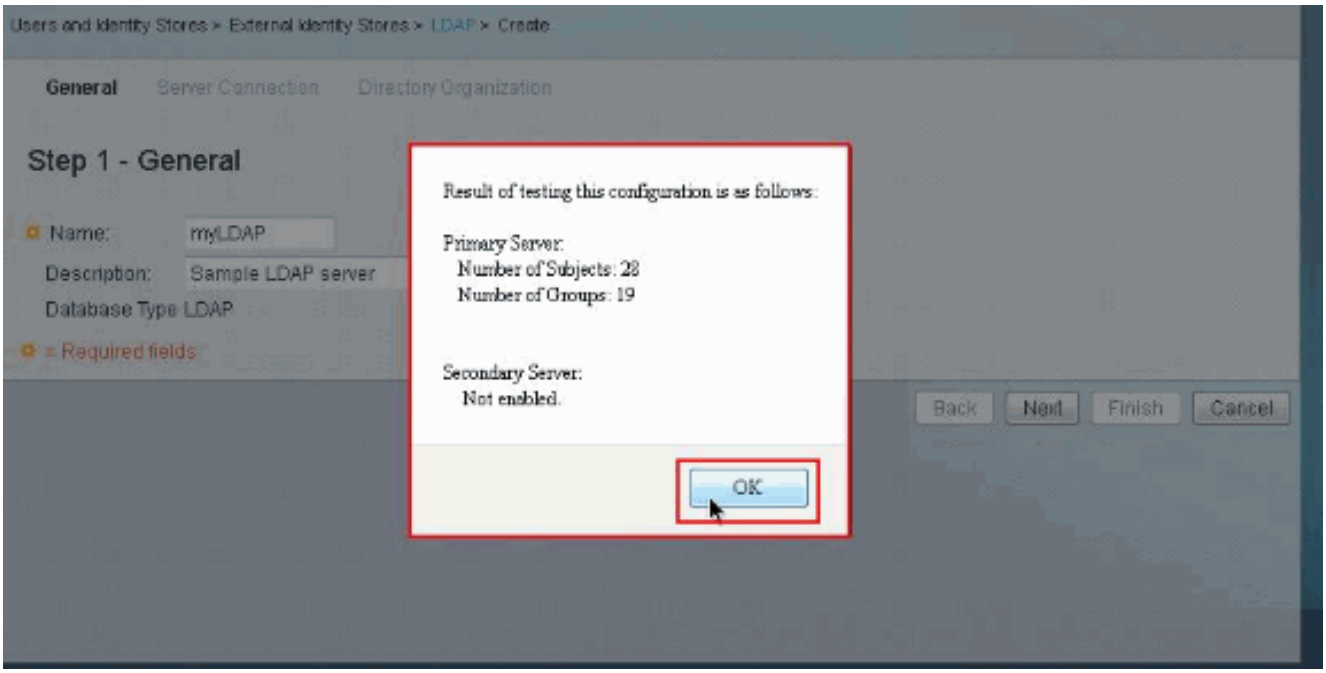
4. انقر فوق **Next (التالي)**.



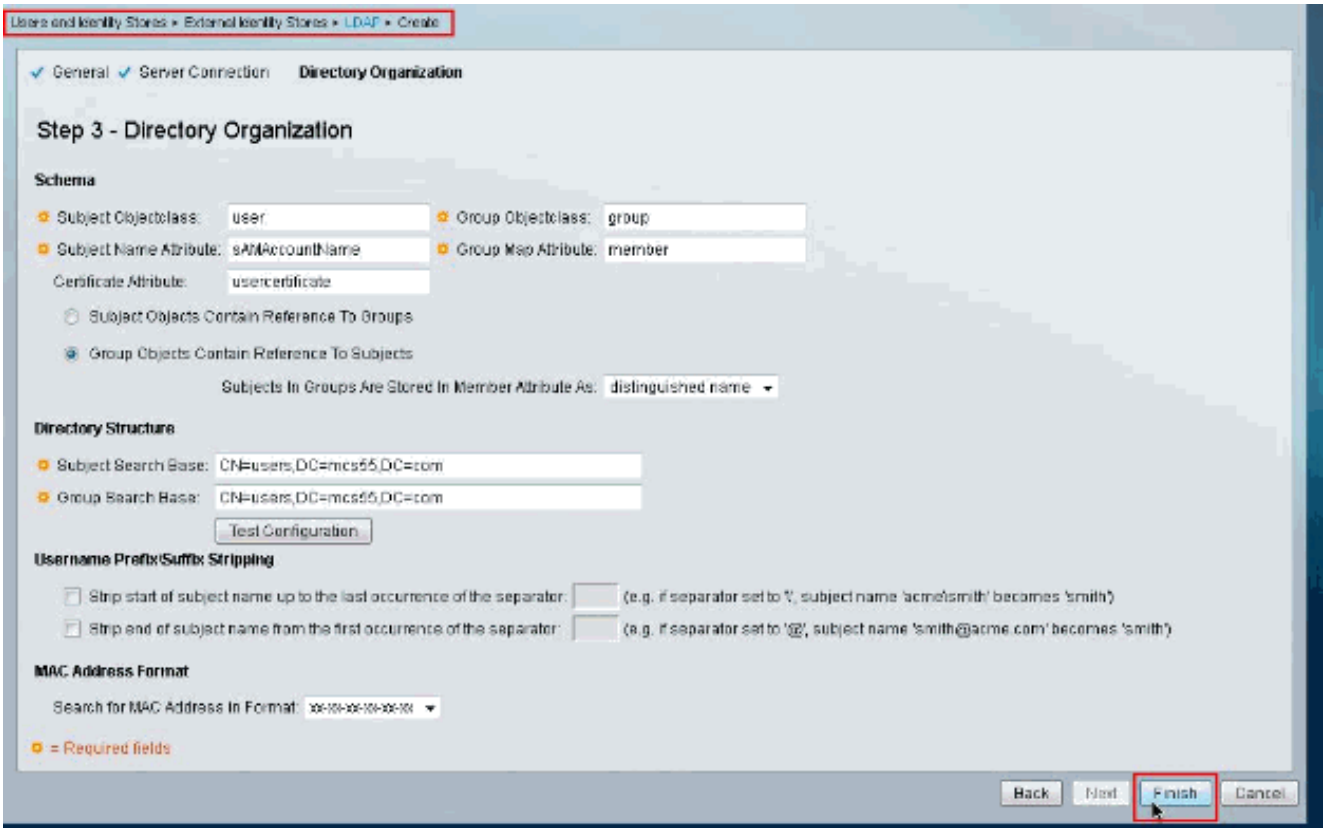
5. من علامة التبويب **مؤسسة الدليل** ضمن قسم **المخطط**، قم بتوفير التفاصيل المطلوبة. وبالمثل، قم بتوفير المعلومات المطلوبة ضمن قسم **بنية الدليل** كما هو موضح من قبل مسؤول LDAP. طقطقة **إختبار تشكيل**.



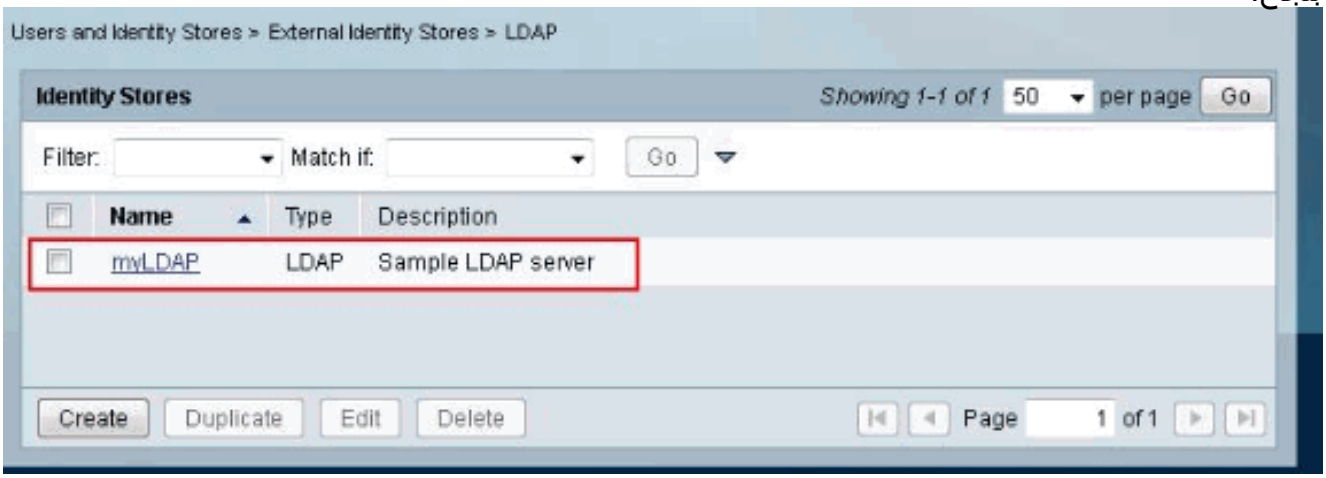
تظهر الصورة التالية أن **إختبار التكوين** ناجح.**ملاحظة:** إذا لم ينجح إختبار التكوين، فأعد التحقق من المعلمات المتوفرة في **المخطط** و**بنية الدليل** من مسؤول LDAP.



6. انقر فوق **إنهاء**.



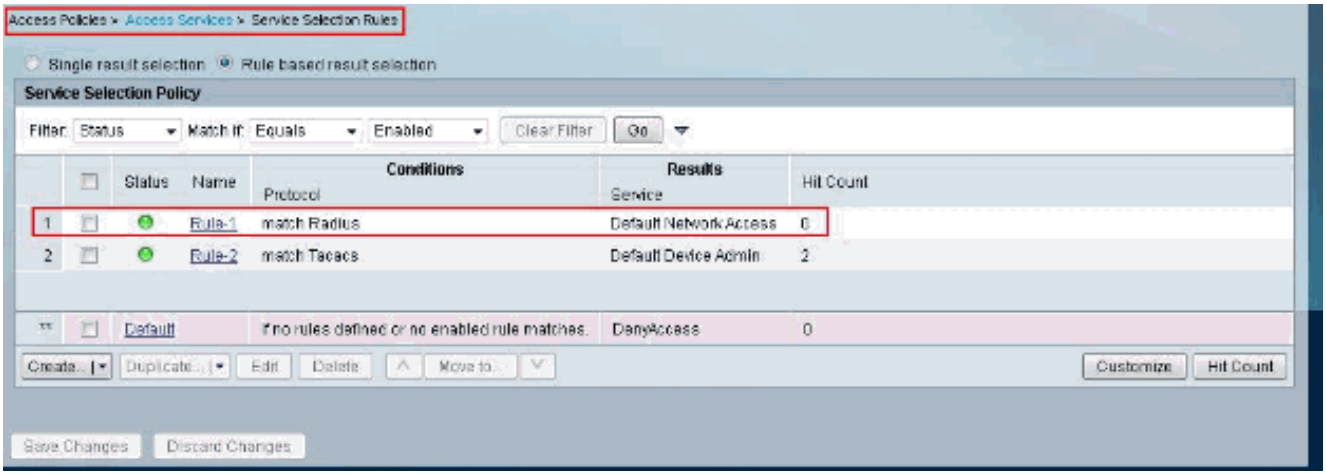
تم إنشاء خادم **LDAP** بنجاح.



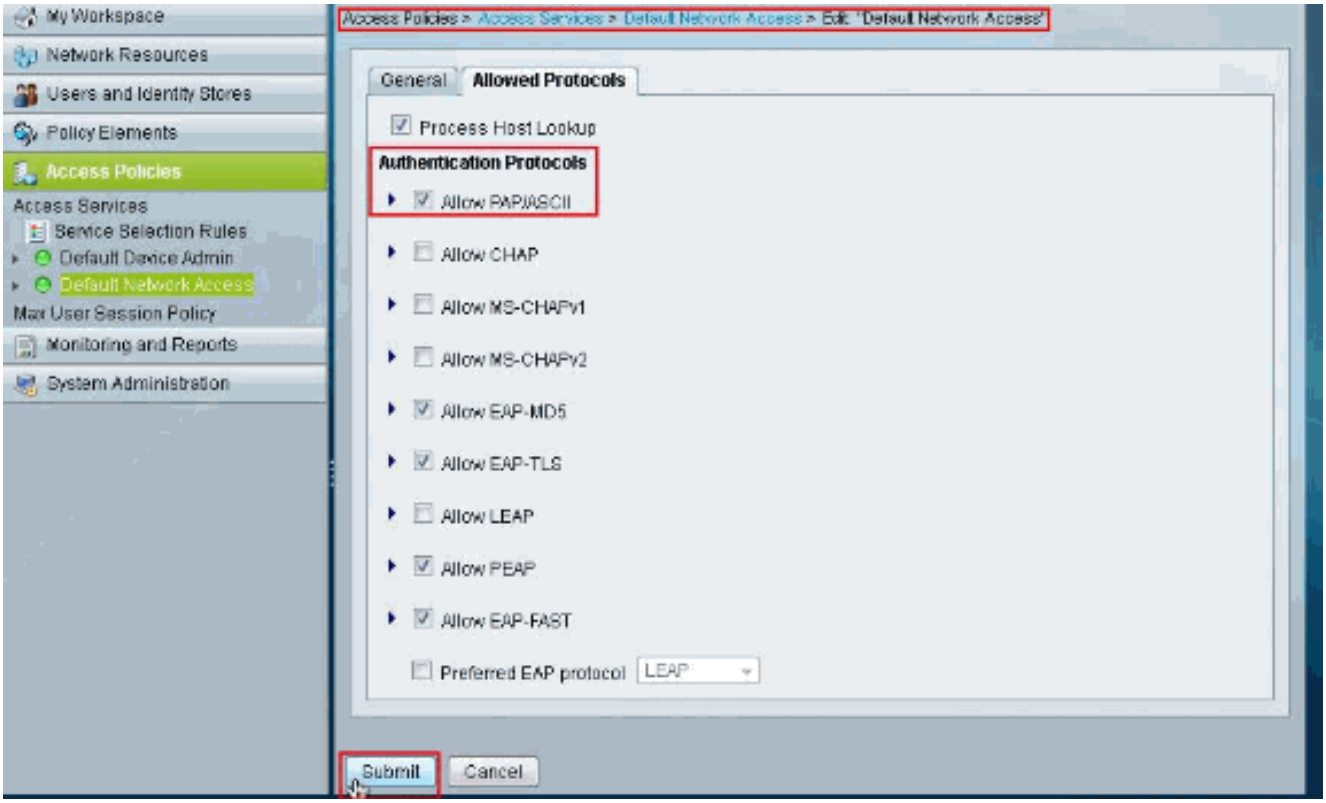
تكوين مخزن الهوية

تنافس هذه الخطوات لتكوين مخزن الهويات:

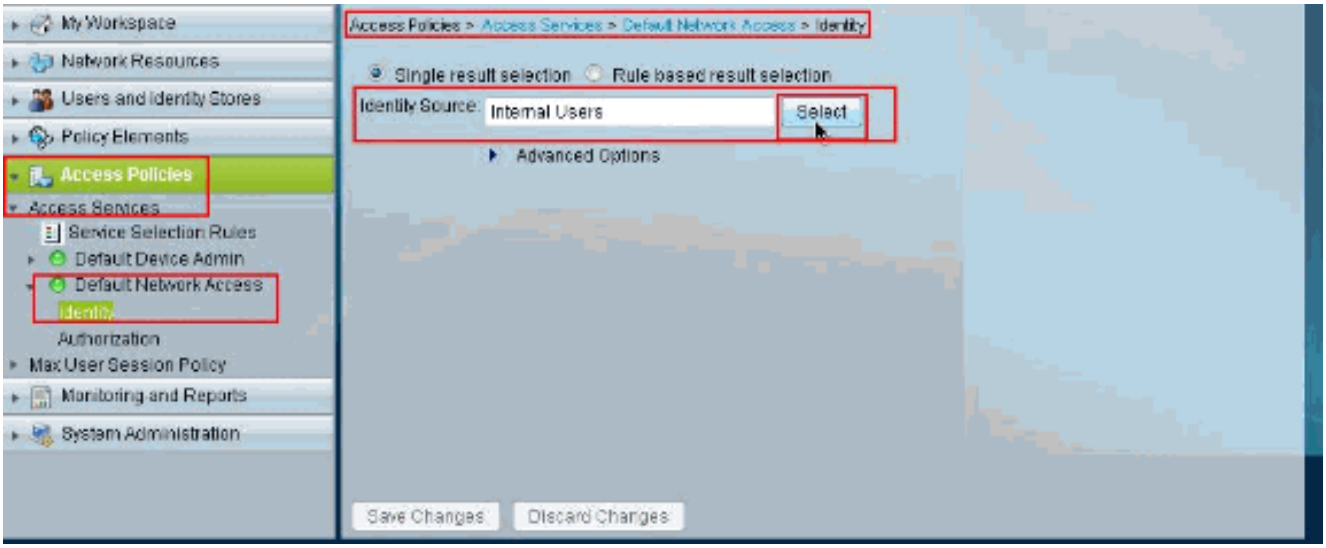
1. أختر **سياسات الوصول > خدمات الوصول > قواعد تحديد الخدمة** وتحقق من الخدمة التي ستستخدم خادم LDAP الآمن للمصادقة. في هذا المثال، تكون الخدمة هي **الوصول الافتراضي للشبكة**.



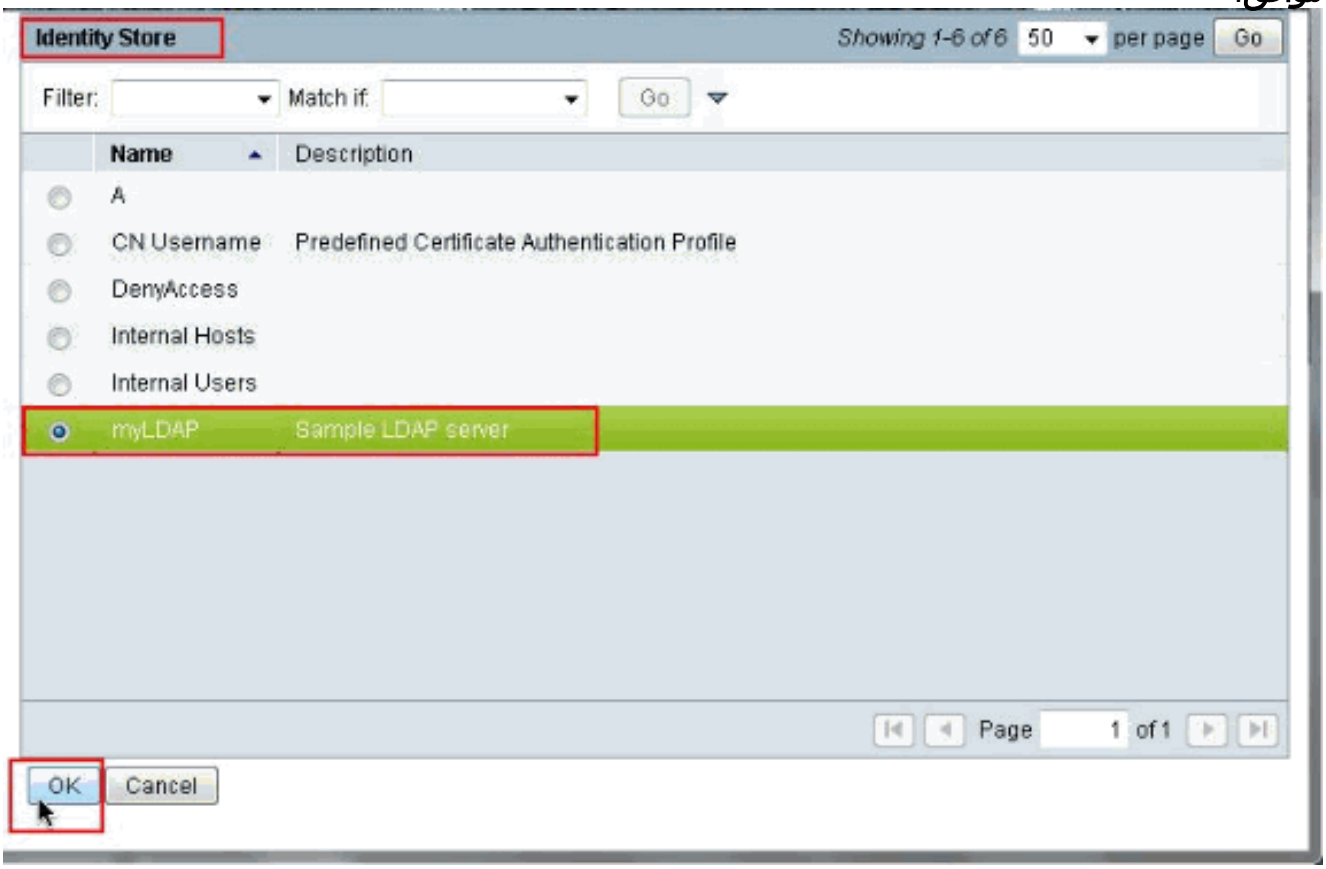
2. بعد التحقق من الخدمة في الخطوة 1، انتقل إلى الخدمة المحددة وانقر فوق **البروتوكولات المسموح بها**. تأكد من تحديد **السماح ب PAP/ASCII**، ثم انقر **إرسال.ملاحظة:** يمكنك تحديد بروتوكولات مصادقة أخرى مع السماح ب
.PAP/ASCII



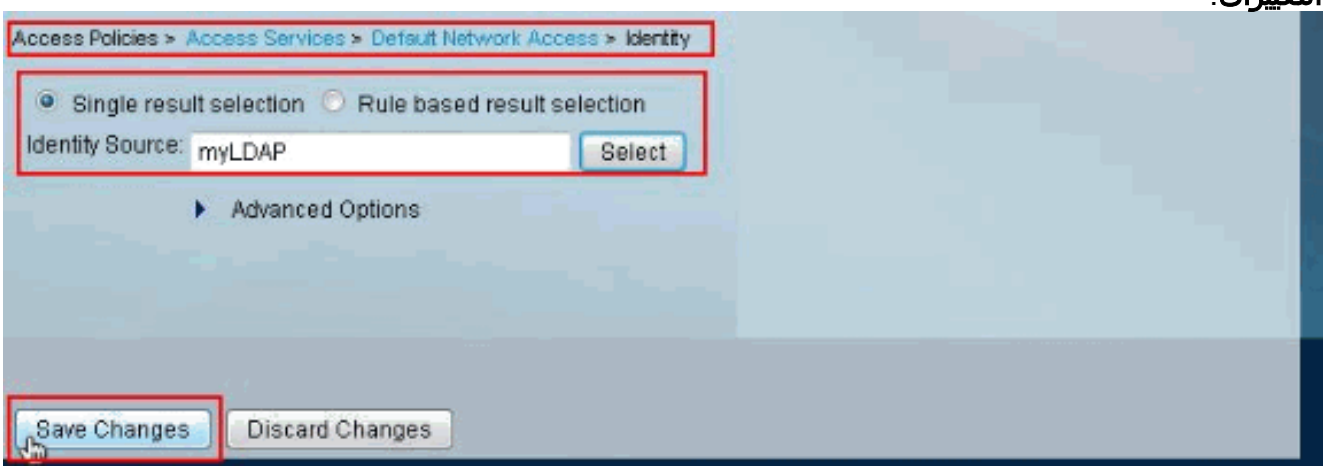
3. انقر فوق الخدمة المحددة في الخطوة 1، ثم انقر فوق **الهوية**. انقر على **تحديد** بجوار **مصدر الهوية**.



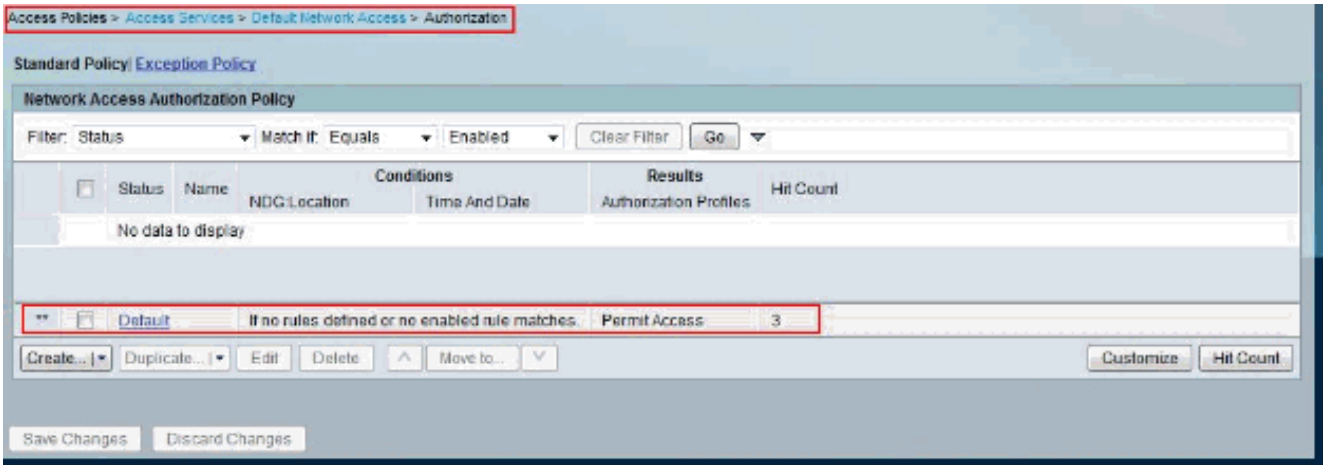
4. حدد **خادم LDAP الآمن** الذي تم إنشاؤه حديثا (**MyLDAP** في هذا المثال)، ثم انقر فوق **موافق**.



5. انقر فوق **حفظ التغييرات**.



6. انتقل إلى قسم **التخويل** في الخدمة المحددة في **الخطوة 1** وتأكد من وجود قاعدة واحدة على الأقل تتيح **المصادقة**.



استكشاف الأخطاء وإصلاحها

يرسل ACS طلب ربط لمصادقة المستخدم مقابل خادم LDAP. يحتوي طلب الربط على DN الخاص بالمستخدم وكلمة مرور المستخدم في نص واضح. تتم مصادقة المستخدم عندما يتطابق DN وكلمة المرور الخاصين بالمستخدم مع اسم المستخدم وكلمة المرور في دليل LDAP.

- **أخطاء المصادقة**— يسجل ACS أخطاء المصادقة في ملفات سجل ACS.
- **أخطاء التهيئة**— أستخدم إعدادات مهلة خادم LDAP لتكوين عدد الثواني التي ينتظرها ACS للحصول على إستجابة من خادم LDAP قبل تحديد فشل الاتصال أو المصادقة على ذلك الخادم. الأسباب المحتملة لخادم LDAP لإرجاع خطأ تهيئة هي:LDAP غير مدعومالخادم معطلنفدت ذاكرة الخادمالمستخدم ليس لديه امتيازاتتم تكوين بيانات اعتماد مسؤول غير صحيحة
- **أخطاء الربط**— الأسباب المحتملة لخادم LDAP لإرجاع أخطاء الربط (المصادقة) هي:أخطاء التصفيةفشل البحث باستخدام معايير المرشحأخطاء المعلمةتم إدخال معلمات غير صحيحةحساب المستخدم مقيد (معطل، مؤمن، منتهي الصلاحية، كلمة المرور منتهية الصلاحية، وهكذا)

يتم تسجيل هذه الأخطاء كأخطاء موارد خارجية، مما يشير إلى وجود مشكلة محتملة مع خادم LDAP:

- حدث خطأ في الاتصال
- انتهت المهلة
- الخادم معطل
- نفدت ذاكرة الخادم

تم تسجيل هذا الخطأ كخطأ مستخدم غير معروف: .

تم تسجيل هذا الخطأ كخطأ كلمة مرور غير صحيح، حيث يوجد المستخدم، ولكن كلمة المرور المرسلة غير صحيحة: .

معلومات ذات صلة

- نظام التحكم في الوصول الآمن من Cisco
- طلبات التعليقات (RFCs)
- 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).