ACS 5.x: مداخ نيوكت لاثم LDAP

المحتويات

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 نظام التحكم بالوصول الآمن (ACS 5.x) من Cisco مع قاعدة بيانات خارجية ل LDAP (تسمى أيضا مخزن الهوية) باستخدام بروتوكول LDAP. هناك طريقتان يستخدمان للاتصال بخادم LDAP: اتصال نص عادي (بسيط) واتصال SSL (مشفر). يمكن تكوين ACS 5.x للاتصال بخادم LDAP باستخدام كلا الطريقتين التاليتين. يقدم هذا المستند مثالا للتكوين لتوصيل ACS 5.x بخادم LDAP باستخدام اتصال بسيط.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن ACS 5.x لديه اتصال IP بخادم LDAP وأن منفذ TCP 389 مفتوح.

بشكل افتراضي، يتم تكوين خادم Microsoft Active Directory LDAP لقبول إتصالات LDAP على منفذ TCP 389. إذا كنت تستخدم أي خادم LDAP آخر، فتأكد من أنه يعمل ويقبل الاتصالات على منفذ TCP 389.

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 برامج أو مجموعة تطبيقات تستخدم لتخزين وتنظيم معلومات حول مستخدمي شبكة الكمبيوتر وموارد الشبكة. يمكنك إستخدام خدمة الدليل لإدارة وصول المستخدم إلى هذه الموارد.

تستند خدمة دليل LDAP إلى طراز عميل-خادم. يتصل العميل بخادم LDAP لبدء جلسة 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 النموذج الموزع لتخزين المعلومات، ويتم عادة نسخ هذه المعلومات نسخا متماثلا 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 يسمى 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 بواسطة ACS لتخويل الأساسي.

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

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، يبلغ مدير الاتصال عن حدوث خطأ أثناء الاتصال الأول للبحث في الدليل، ويحاول تجديد الاتصال.

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

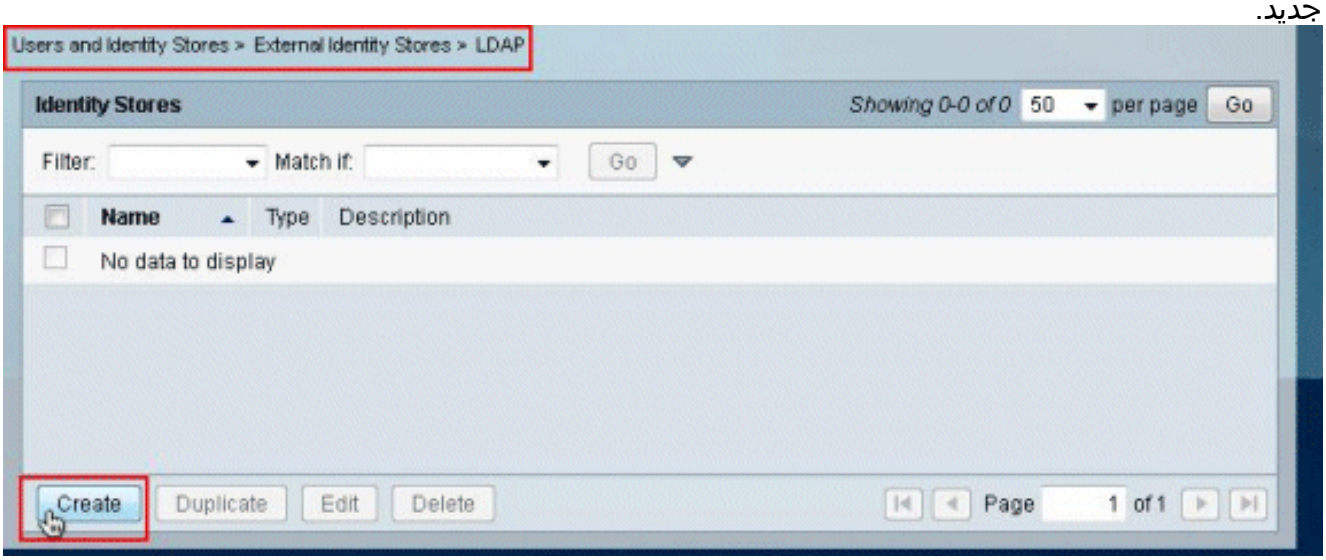
التكوين

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

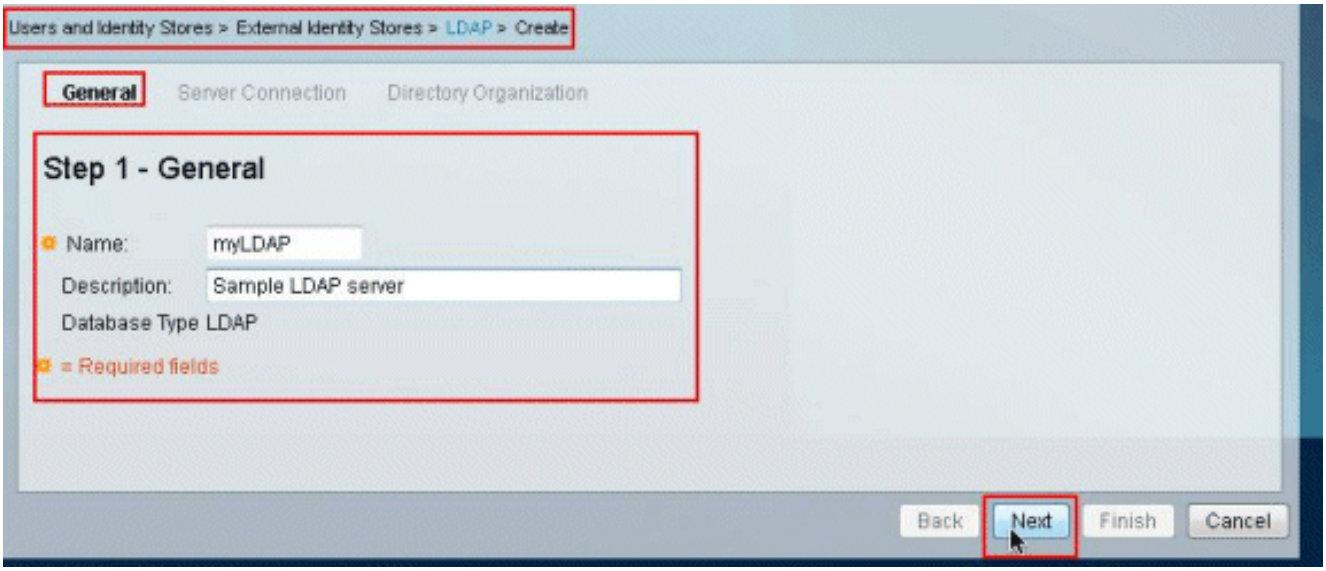
تكوين ACS 5.x ل LDAP

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

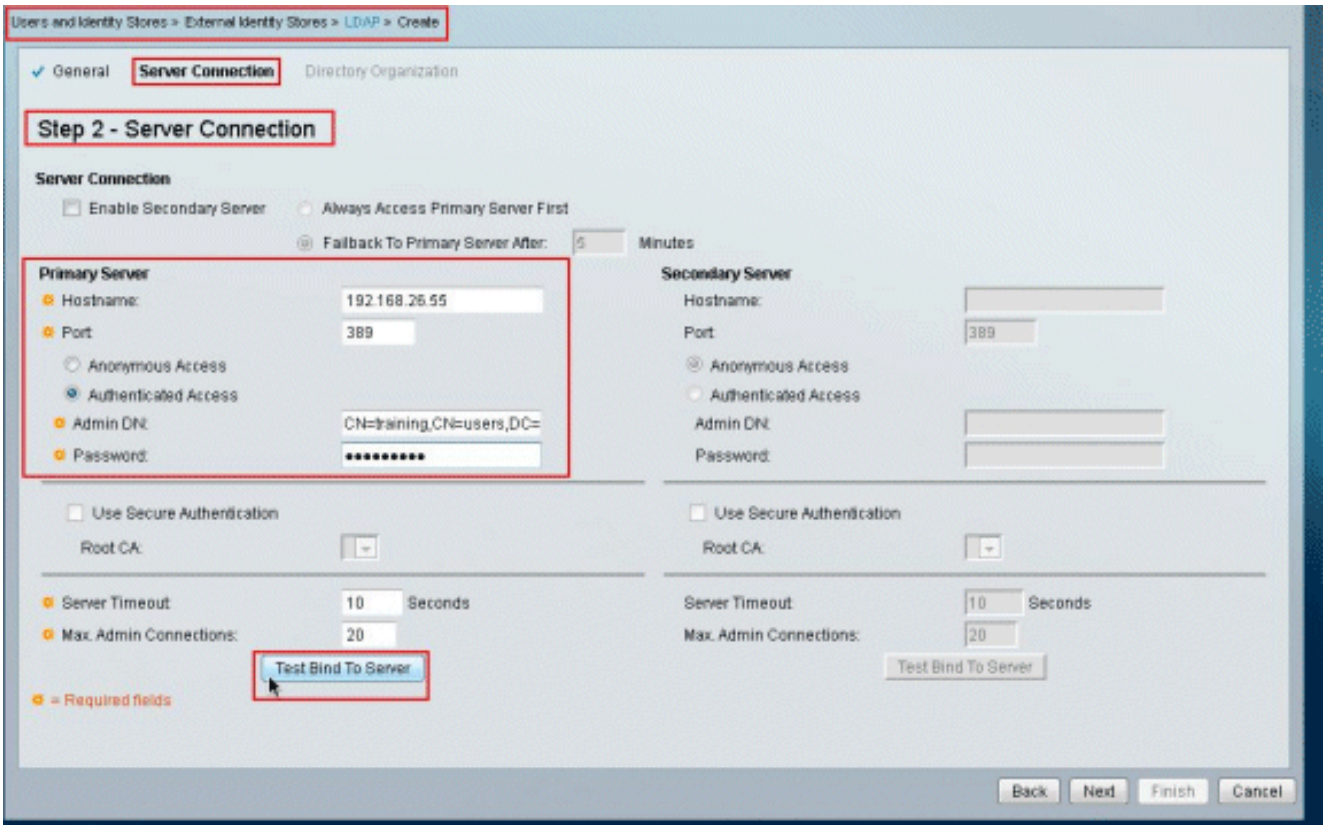
1. أخترت **مستخدمين ومتاجر هوية>خارجي هوية يخزن>LDAP**، وطقطقة **يخلق** in order to خلقت توصيل LDAP جديد.



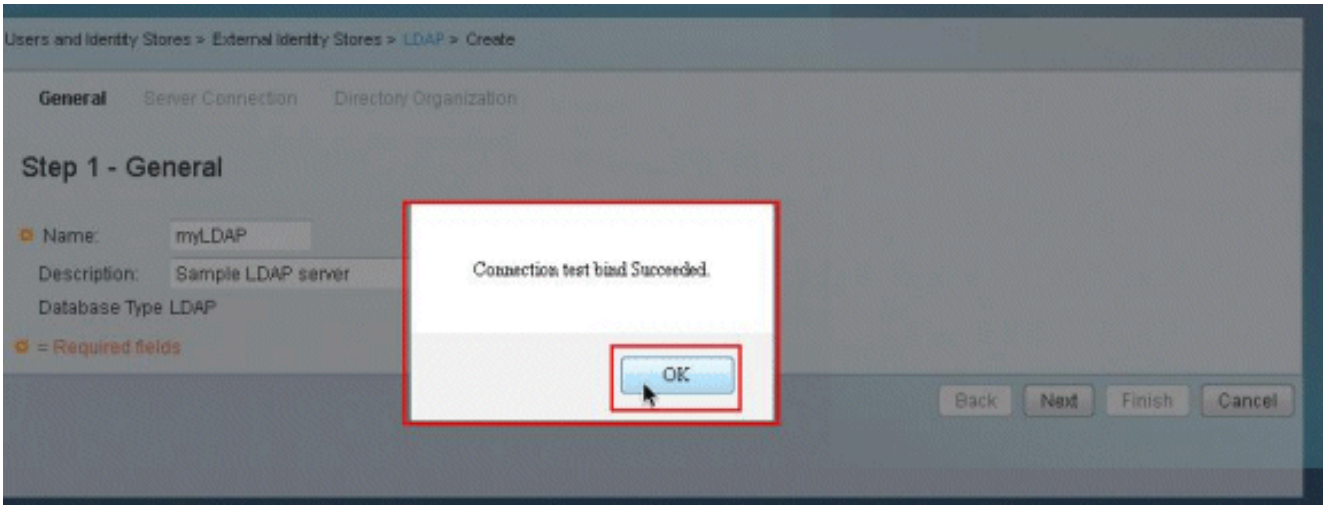
2. في علامة التبويب "عام"، قم بتوفير **الاسم** و**الوصف** (إختياري) ل LDAP الجديد، وانقر فوق **التالي**.



3. في علامة التبويب اتصال الخادم الموجودة ضمن القسم "الخادم الأساسي"، قم بتوفير **اسم المضيف** و**المنفذ** و**Admin DN** و**كلمة المرور**. انقر فوق **إختبار الربط بالخادم**.**ملاحظة:** رقم المنفذ المعين ل LDAP في ANA هو TCP 389. ومع ذلك، قم بتأكيد رقم المنفذ الذي يستخدمه خادم LDAP من مسؤول LDAP. يجب أن يتم توفير DN للمسؤول وكلمة المرور لك بواسطة مسؤول LDAP الخاص بك. يجب أن يكون لدى Admin DN الخاص بك كافة الأذونات على كافة وحدات التحكم على خادم LDAP.

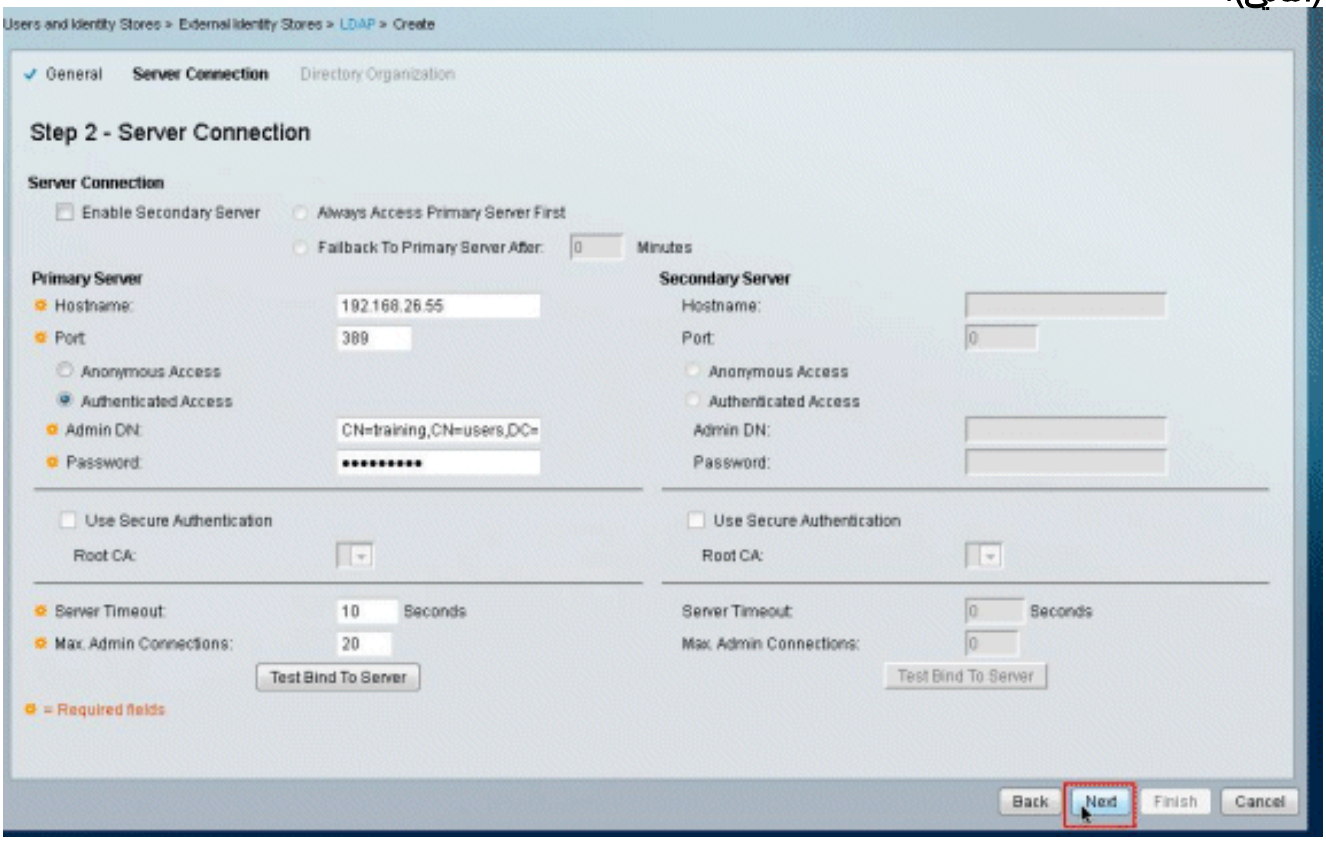


4. توضح هذه الصورة أن **ربط إختبار الاتصال بالخادم** تم بنجاح.

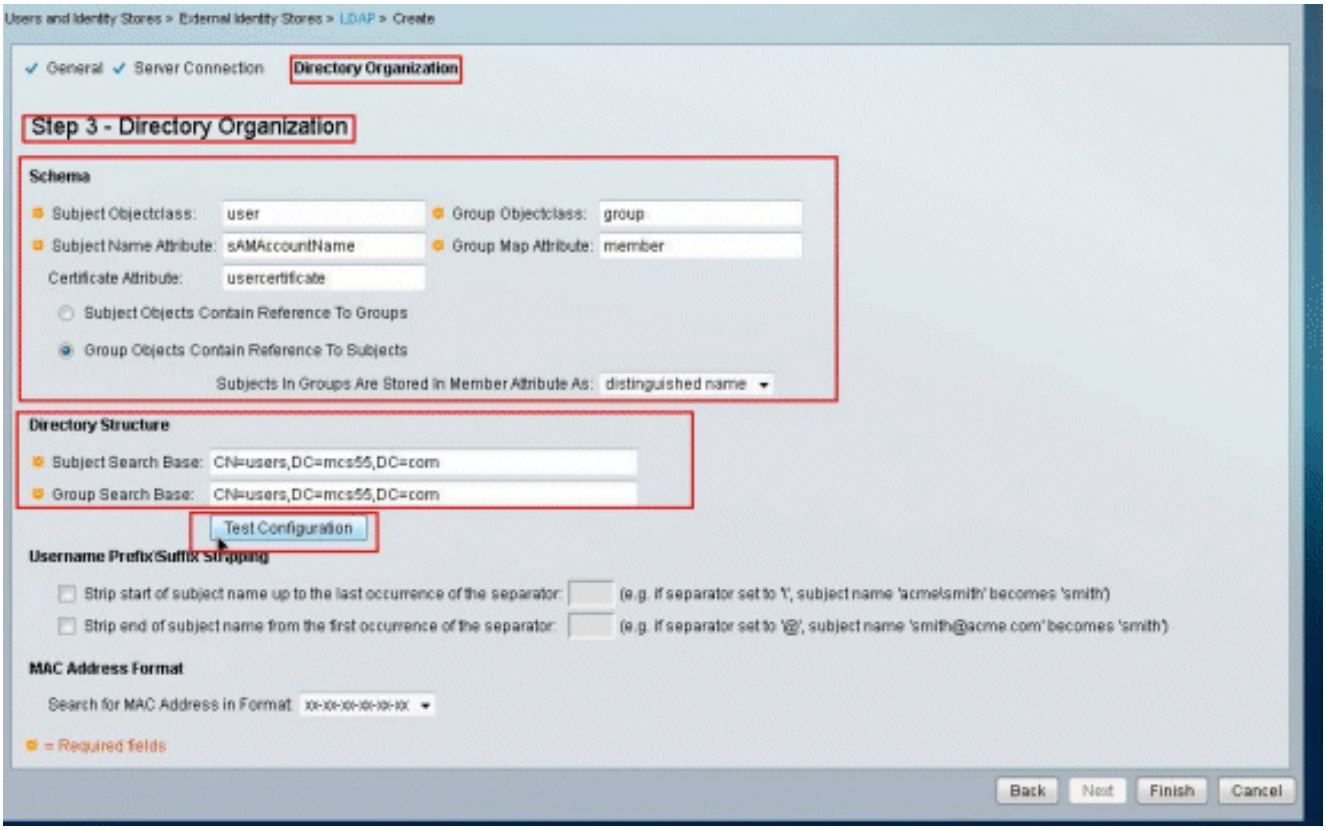


ملاحظة: إذا لم ينجح إختبار الربط، فأعد التحقق من **اسم المضيف**، و**رقم المنفذ**، و**Admin DN**، و**كلمة المرور** من مسؤول LDAP الخاص بك.

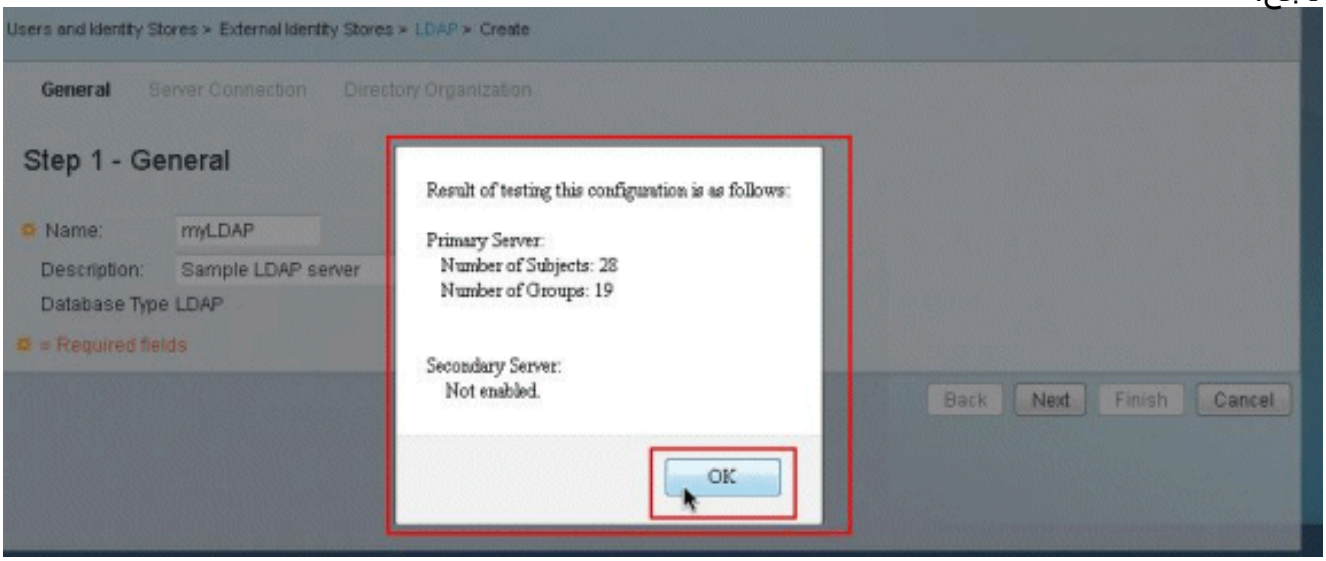
5. انقر فوق **Next (التالي)**.



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

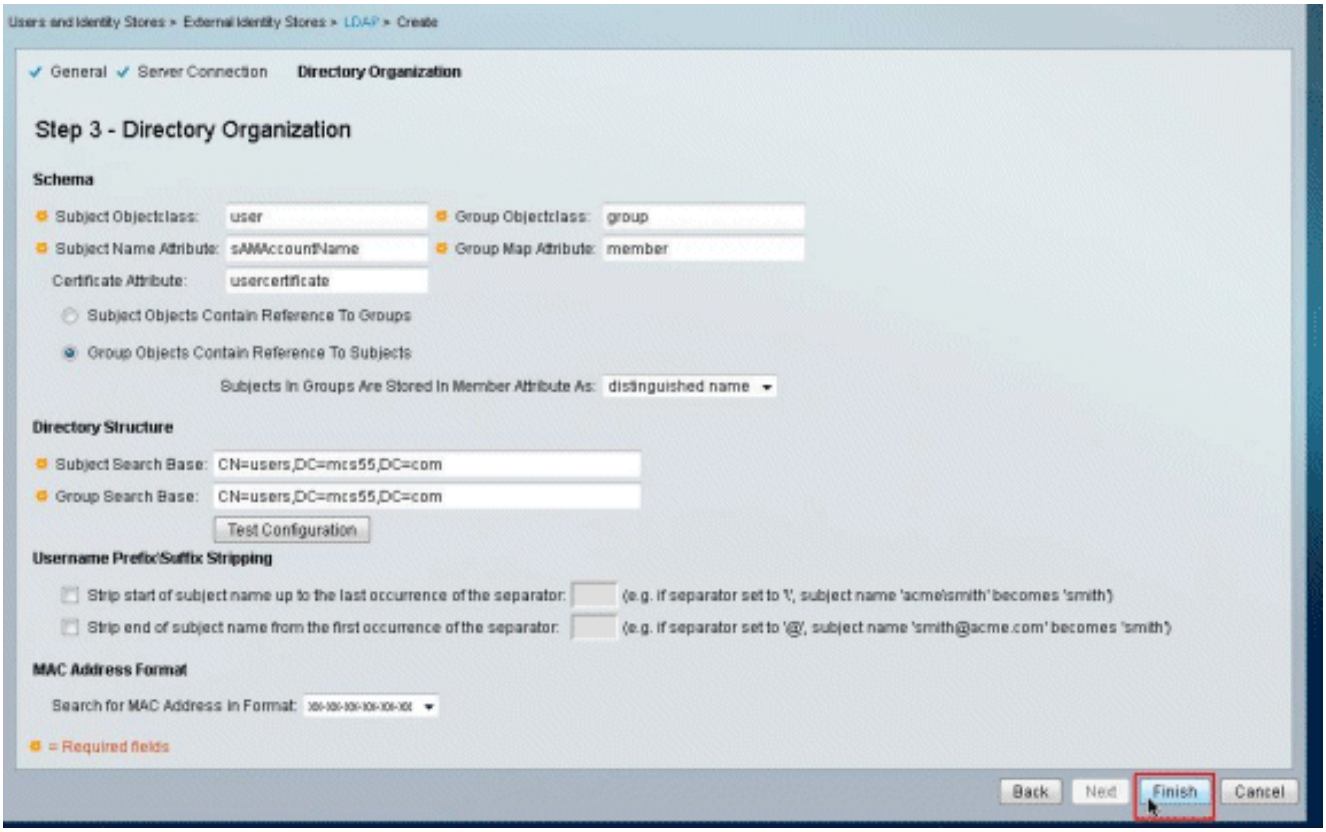


7. توضح هذه الصورة أن **إختبار التكوين** ناجح.

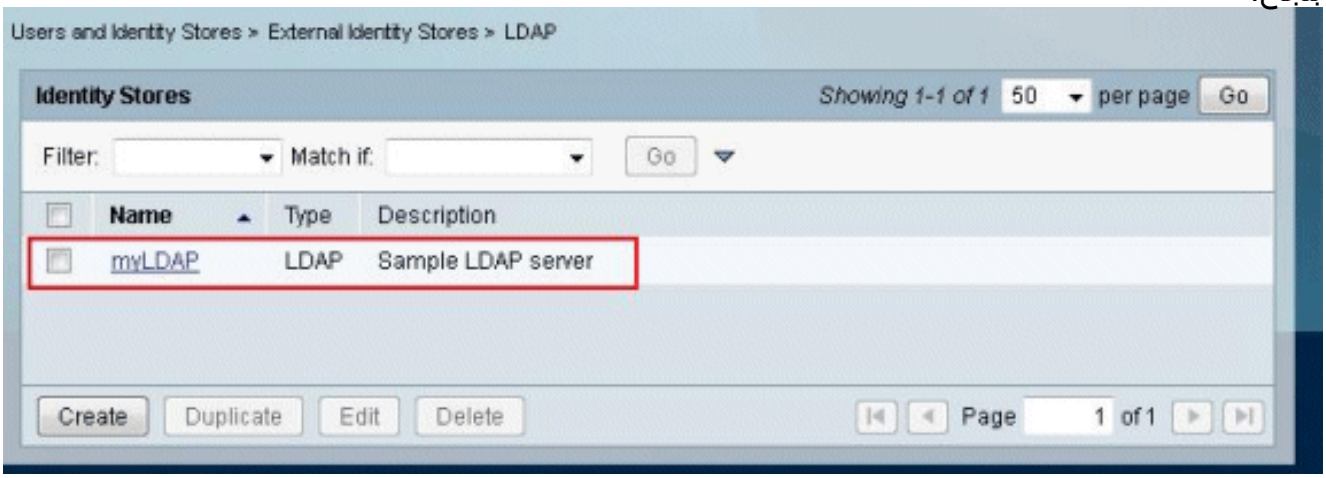


ملاحظة: إذا لم ينجح إختبار التكوين، أعد التحقق من المعلمات المتوفرة في **المخطط** و**بنية الدليل** من مسؤول LDAP.

8. انقر فوق **إنهاء**.



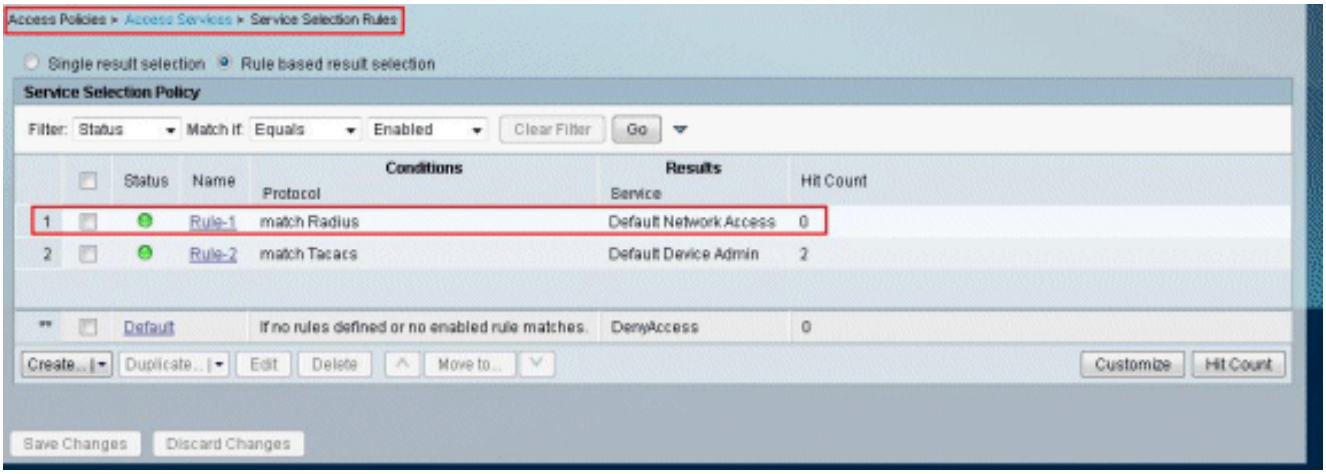
9. تم إنشاء خادم **LDAP** بنجاح.



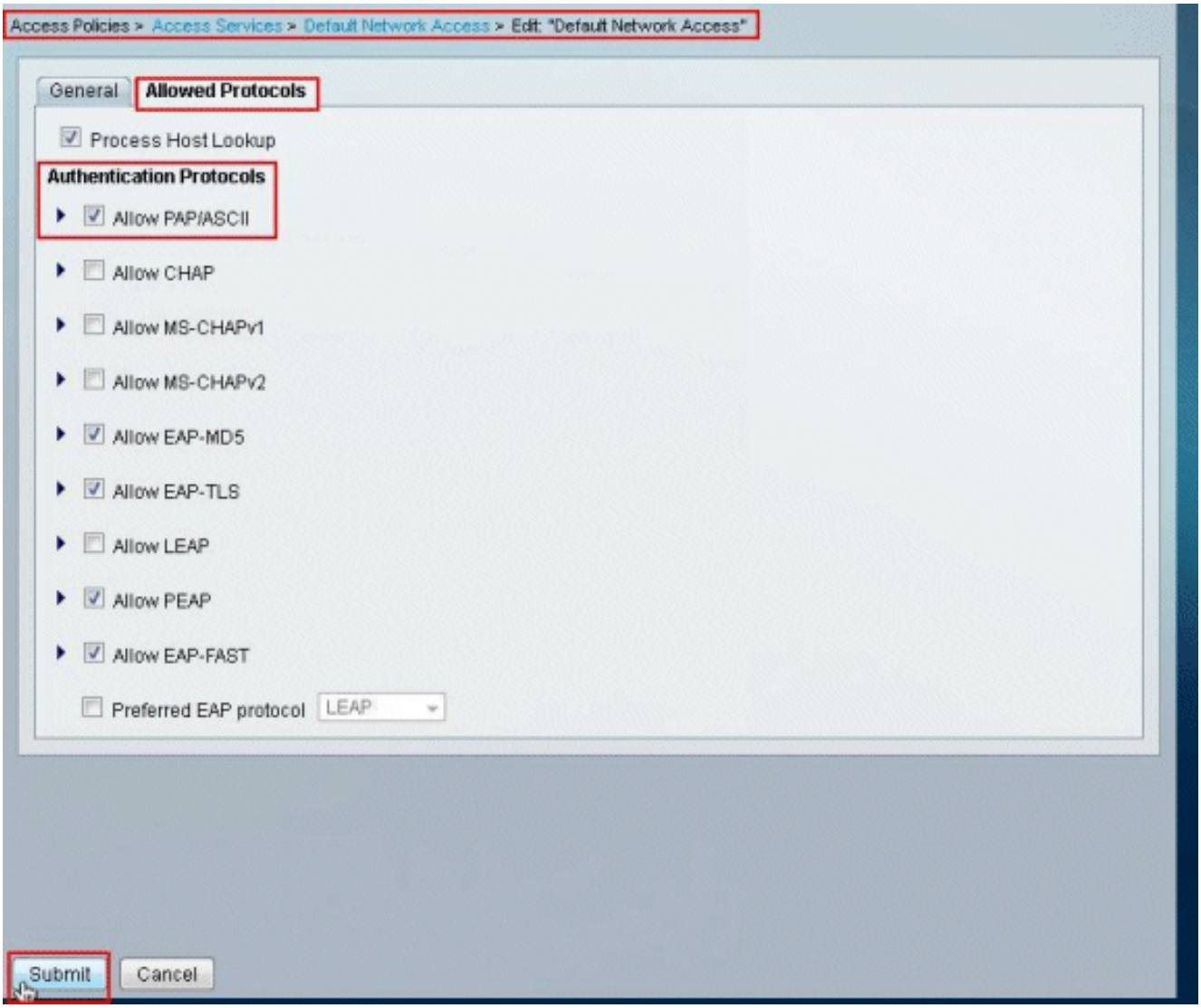
تكوين مخزن الهوية

تنافس الخطوات لتكوين مخزن الهويات:

1. أختر **سياسات الوصول** > **خدمات الوصول** > **قواعد تحديد الخدمة**، وتحقق من الخدمة التي ستستخدم خادم LDAP للمصادقة. في هذا المثال، تستخدم مصادقة خادم LDAP خدمة **الوصول إلى الشبكة الافتراضية**.

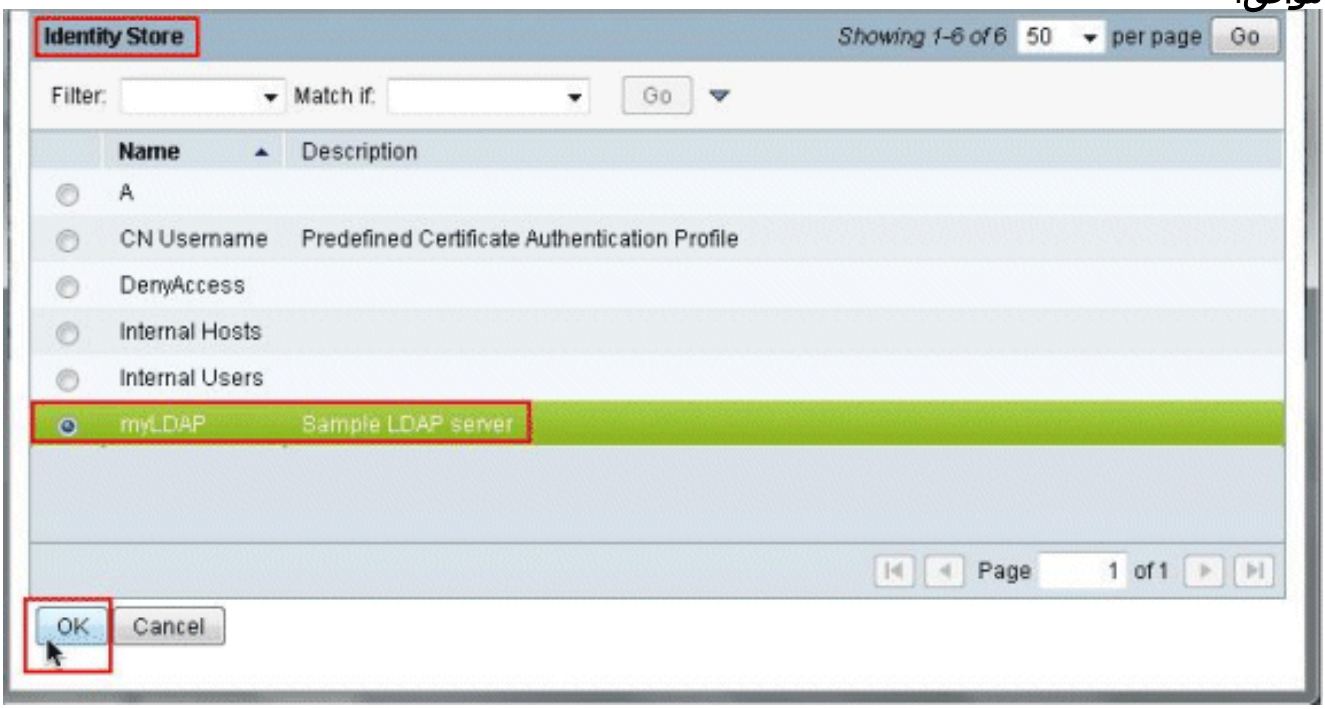


2. بمجرد التحقق من الخدمة في الخطوة 1، انتقل إلى الخدمة المحددة وانقر فوق **البروتوكولات المسموح بها**. تأكد من تحديد **السماح ب PAP/ASCII**، وانقر **إرسال**.**ملاحظة:** يمكنك تحديد بروتوكولات مصادقة أخرى مع السماح ب PAP/ASCII.

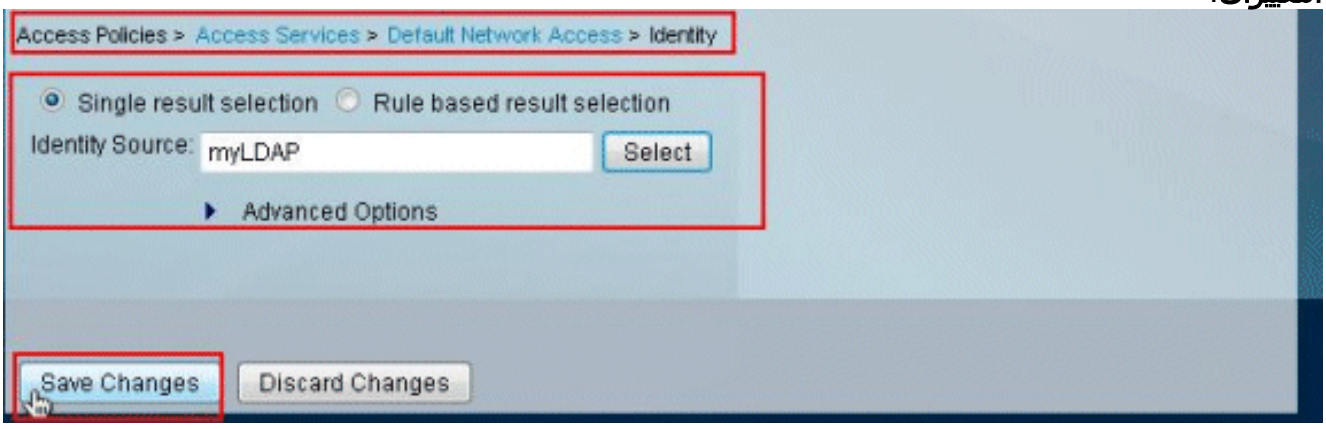


3. انقر فوق الخدمة المحددة في الخطوة 1، ثم انقر فوق **الهوية**. انقر فوق **تحديد** إلى يمين حقل مصدر الهوية.

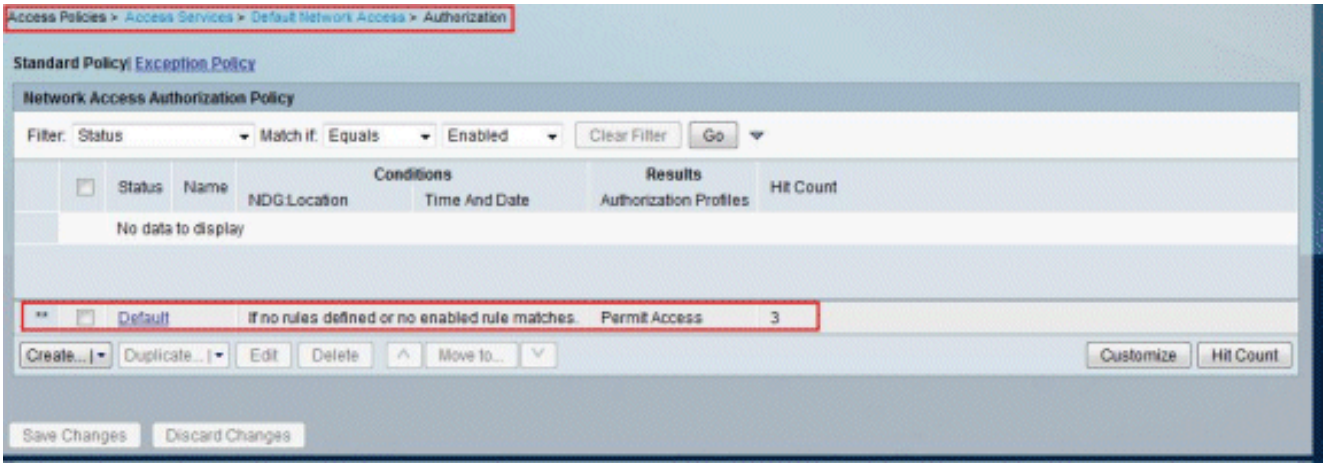
4. حدد خادم LDAP الذي تم إنشاؤه حديثا (**MyLDAP**، في هذا المثال)، وانقر فوق **موافق**.



5. انقر فوق **حفظ التغييرات**.



6. انتقل إلى قسم التخويل في الخدمة المحددة في الخطوة 1، وتأكد من وجود قاعدة واحدة على الأقل تسمح **بالمصادقة**.



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 للاستجابة 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

المستخدم خطأ تم تسجيله كخطأ مستخدم غير معروف.

تم تسجيل خطأ 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).