

LDAP مداخل نيوكت لاثم ACS 5.x

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [معلومات أساسية](#)
- [خدمة Directory](#)
- [المصادقة باستخدام LDAP](#)
- [إدارة اتصال LDAP](#)
- [التكوين](#)
- [تكوين ACS 5.x ل LDAP](#)
- [تكوين مخزن الهوية](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [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 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 مثلا 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 استخدام 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 نسخاً متماثلاً 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 نسخاً متماثلاً 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، متبوعاً بـ DN الخاص بالإدخال الأصل. يمكنك التفكير في DN كاسم ملف كامل، و RDN كاسم ملف نسبي في مجلد.

المصادقة باستخدام LDAP

يمكن لـ 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 لـ ACS إستراداد المجموعات والسمات التي تنتمي إلى الأساسي. يمكن تكوين السمات المطلوب إسترادادها في واجهة ويب ACS (صفحات LDAP). يمكن استخدام هذه المجموعات والسمات بواسطة ACS لتحويل 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 اتصالات 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 مقدماً 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 بمدير الاتصال. أحلت ل كثير معلومة، [ACS 5.x](#) [مستعمل مرشد](#).

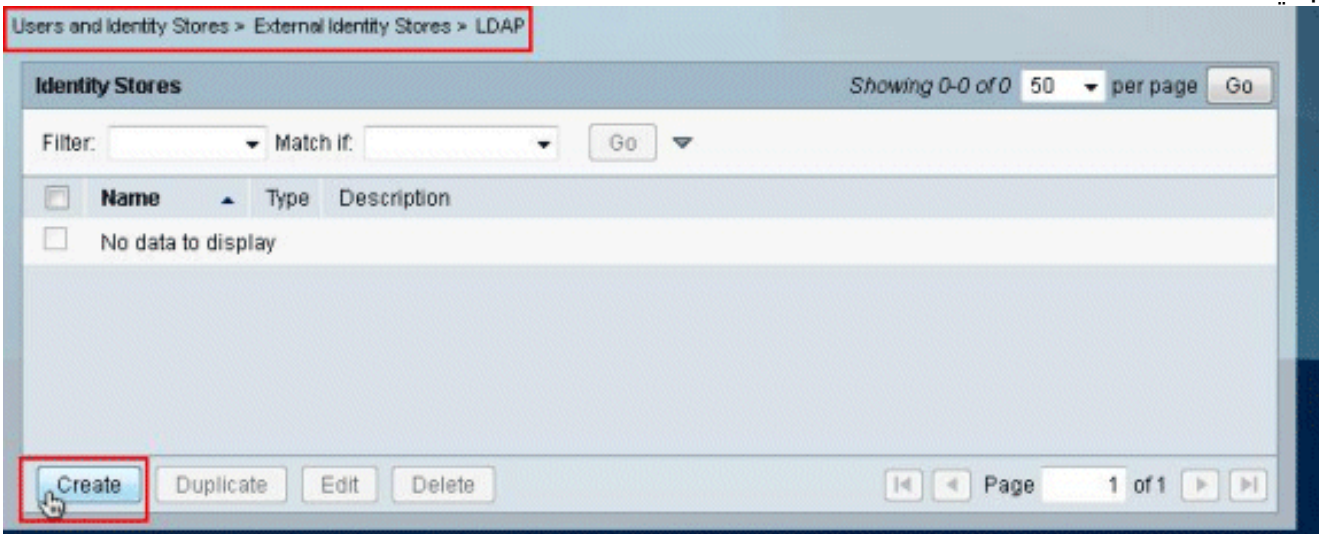
التكوين

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. أختارت **مستخدمين ومناجر هوية > خارجي هوية يخزن > LDAP**، وطققة **يخلق** in order to خلقت توصيل LDAP جديد.



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

Users and Identity Stores > External Identity Stores > LDAP > Create

General Server Connection Directory Organization

Step 1 - General

Name: myLDAP
 Description: Sample LDAP server
 Database Type LDAP

= Required fields

Back Next Finish Cancel

3. في علامة التبويب اتصال الخادم الموجودة ضمن القسم "الخادم الأساسي"، قم بتوفير اسم المضيف والمنفذ و Admin DN وكلمة المرور. انقر فوق إختبار الربط بالخادم. ملاحظة: رقم المنفذ المعين ل LDAP في ANA هو 389 TCP. 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.

Users and Identity Stores > External Identity Stores > LDAP > Create

General **Server Connection** Directory Organization

Step 2 - Server Connection

Server Connection

Enable Secondary Server Always Access Primary Server First
 Fallback To Primary Server After: 5 Minutes

Primary Server

Hostname: 192.168.26.55
 Port: 389
 Anonymous Access
 Authenticated Access
 Admin DN: CN=training,CN=users,DC=
 Password: *****

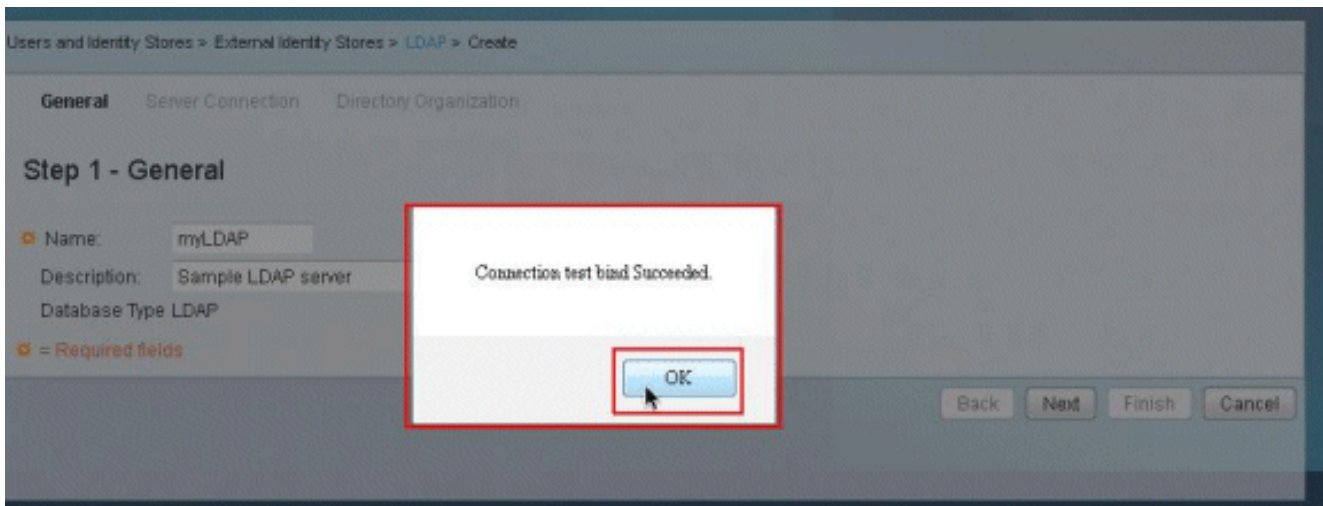
Use Secure Authentication
 Root CA: [v]

Server Timeout: 10 Seconds
 Max. Admin Connections: 20
 Test Bind To Server

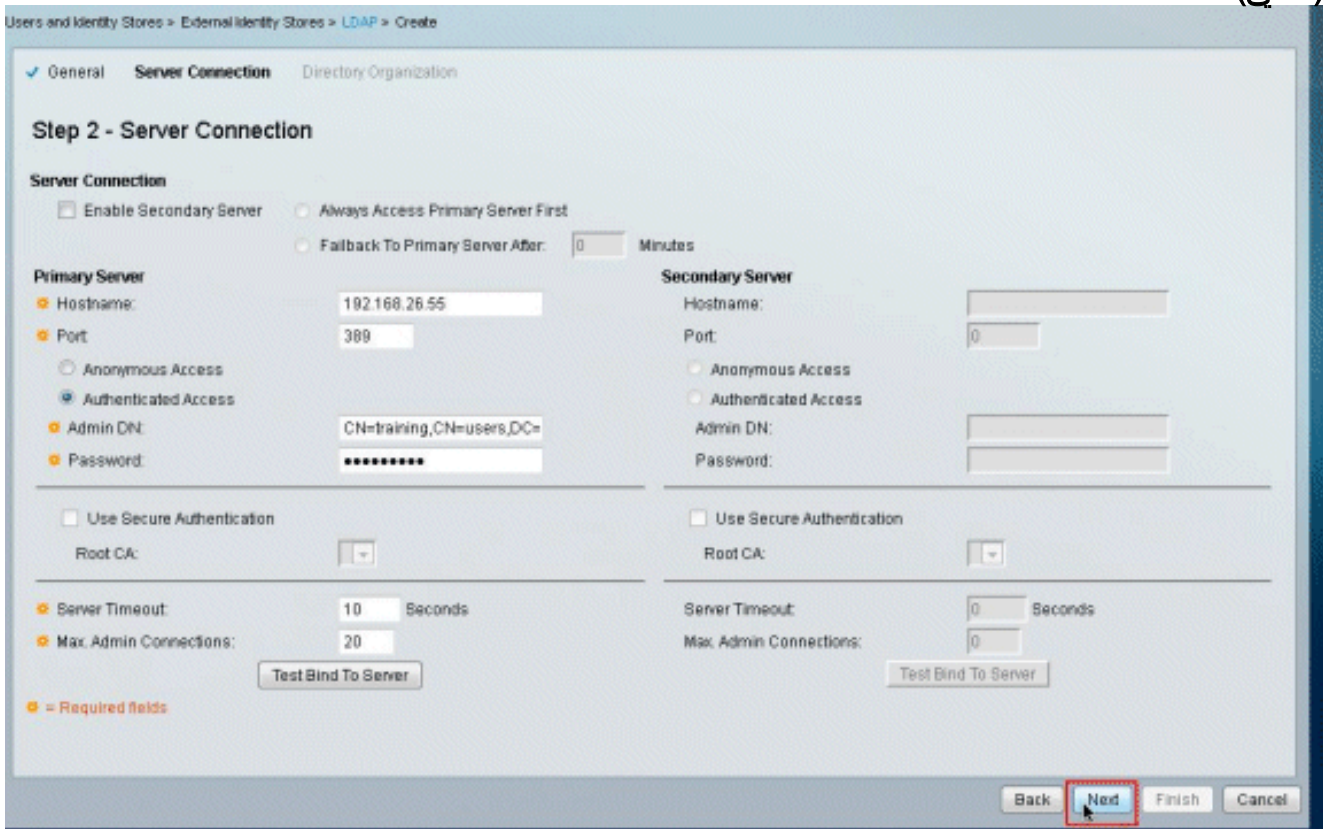
= Required fields

Back Next Finish Cancel

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



ملاحظة: إذا لم ينجح إختبار الربط، فأعد التحقق من اسم المضيف، ورقم المنفذ، وAdmin DN، وكلمة 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.

Users and Identity Stores > External Identity Stores > LDAP > Create

General Server Connection **Directory Organization**

Step 3 - Directory Organization

Schema

Subject Objectclass: user Group Objectclass: group
 Subject Name Attribute: sAMAccountName Group Map Attribute: member
 Certificate Attribute: usercertificate
 Subject Objects Contain Reference To Groups
 Group Objects Contain Reference To Subjects
 Subjects In Groups Are Stored In Member Attribute As: distinguished name

Directory Structure

Subject Search Base: CN=users,DC=mcs55,DC=com
 Group Search Base: CN=users,DC=mcs55,DC=com

Test Configuration

Username Prefix/Suffix Stripping

Strip start of subject name up to the last occurrence of the separator: (e.g. if separator set to '\', subject name 'acme\smith' becomes 'smith')
 Strip end of subject name from the first occurrence of the separator: (e.g. if separator set to '@', subject name 'smith@acme.com' becomes 'smith')

MAC Address Format

Search for MAC Address in Format: xx-xx-xx-xx-xx-xx

Required fields

Back Next Finish Cancel

7. توضح هذه الصورة أن إختبار التكوين ناجح.

Users and Identity Stores > External Identity Stores > LDAP > Create

General Server Connection Directory Organization

Step 1 - General

Name: myLDAP
 Description: Sample LDAP server
 Database Type: LDAP

Required fields

Result of testing this configuration is as follows:

Primary Server:
 Number of Subjects: 28
 Number of Groups: 19

Secondary Server:
 Not enabled.

Back Next Finish Cancel

OK

ملاحظة: إذا لم ينجح إختبار التكوين، أعد التحقق من المعلمات المتوفرة في المخطط وبنية الدليل من مسؤول LDAP.
 8. انقر فوق إنهاء.

Users and Identity Stores > External Identity Stores > LDAP > Create

General Server Connection **Directory Organization**

Step 3 - Directory Organization

Schema

Subject Objectclass: user Group Objectclass: group
 Subject Name Attribute: sAMAccountName Group Map Attribute: member
 Certificate Attribute: usercertificate

Subject Objects Contain Reference To Groups
 Group Objects Contain Reference To Subjects
 Subjects in Groups Are Stored In Member Attribute As: distinguished name

Directory Structure

Subject Search Base: CN=users,DC=mcs55,DC=com
 Group Search Base: CN=users,DC=mcs55,DC=com

Username Prefix/Suffix Stripping

Strip start of subject name up to the last occurrence of the separator: (e.g. if separator set to '\', subject name 'acme\smith' becomes 'smith')
 Strip end of subject name from the first occurrence of the separator: (e.g. if separator set to '@', subject name 'smith@acme.com' becomes 'smith')

MAC Address Format

Search for MAC Address In Format: xx-xx-xx-xx-xx-xx

Required fields

Back Next **Finish** Cancel

9. تم إنشاء خادم LDAP بنجاح.

Users and Identity Stores > External Identity Stores > LDAP

Identity Stores Showing 1-1 of 1 50 per page Go

Filter: Match if: Go

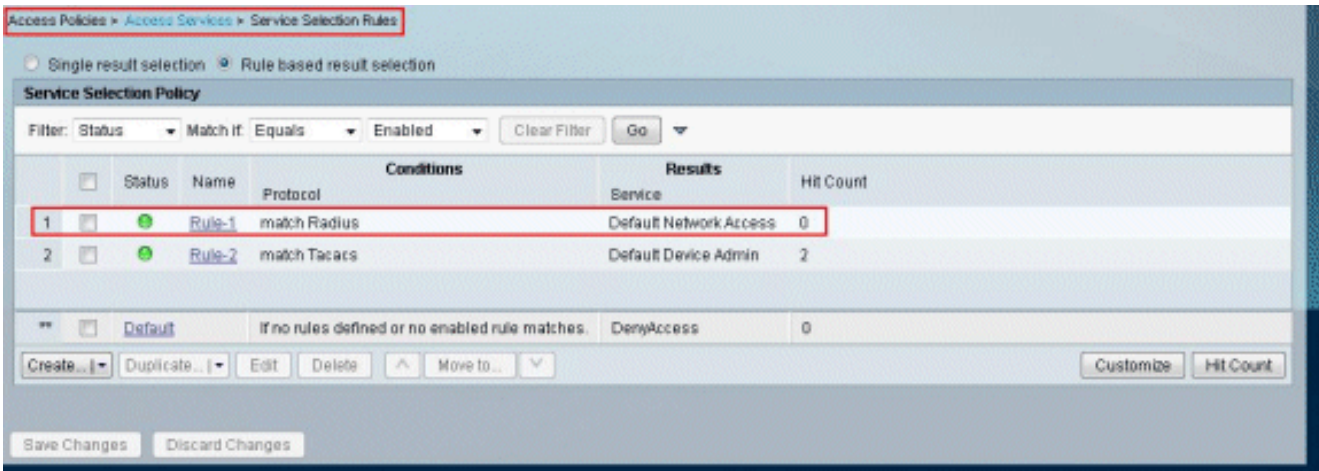
Name	Type	Description
myLDAP	LDAP	Sample LDAP server

Create Duplicate Edit Delete Page 1 of 1

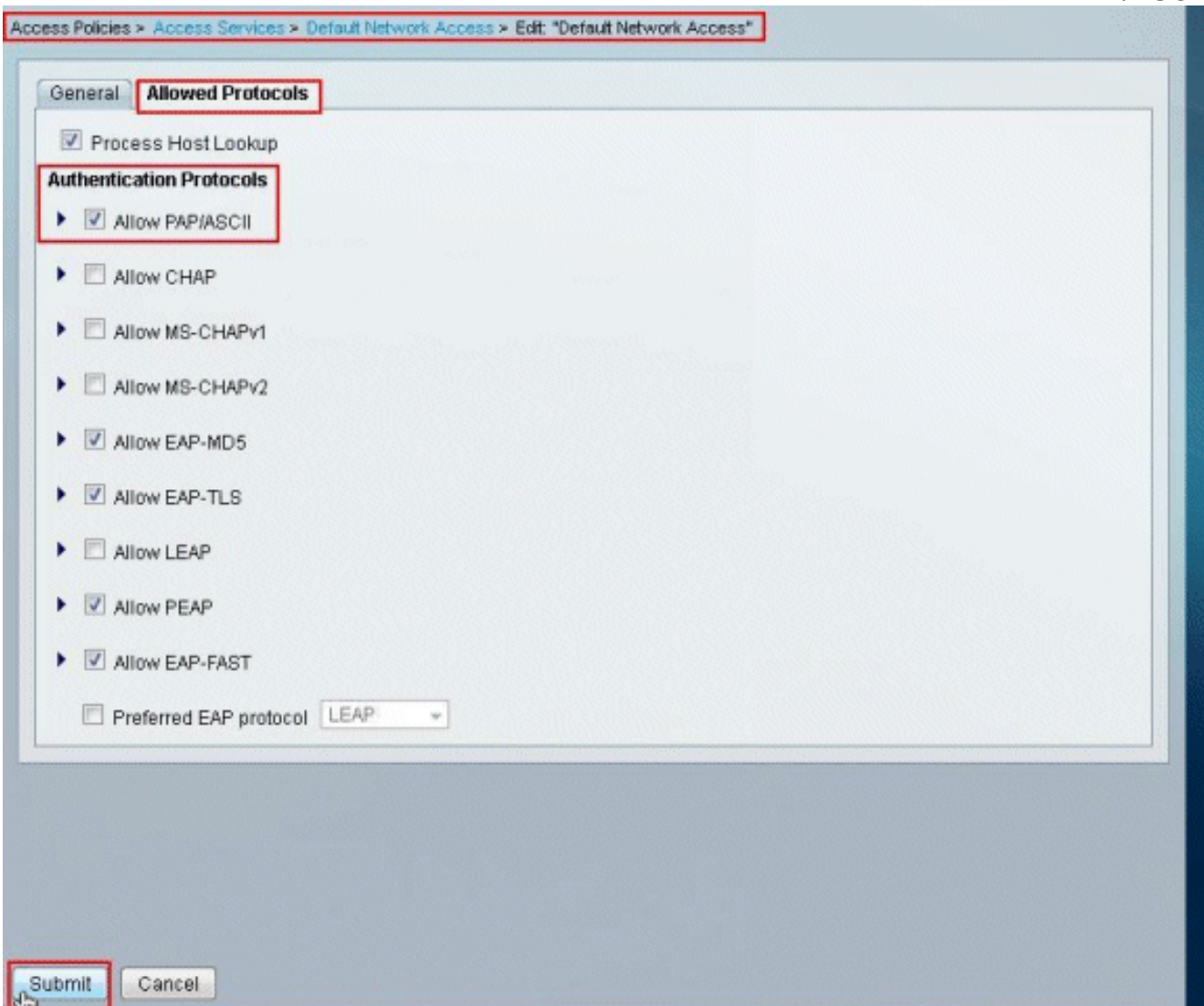
تكوين مخزن الهوية

تتألف الخطوات لتكوين مخزن الهويات:

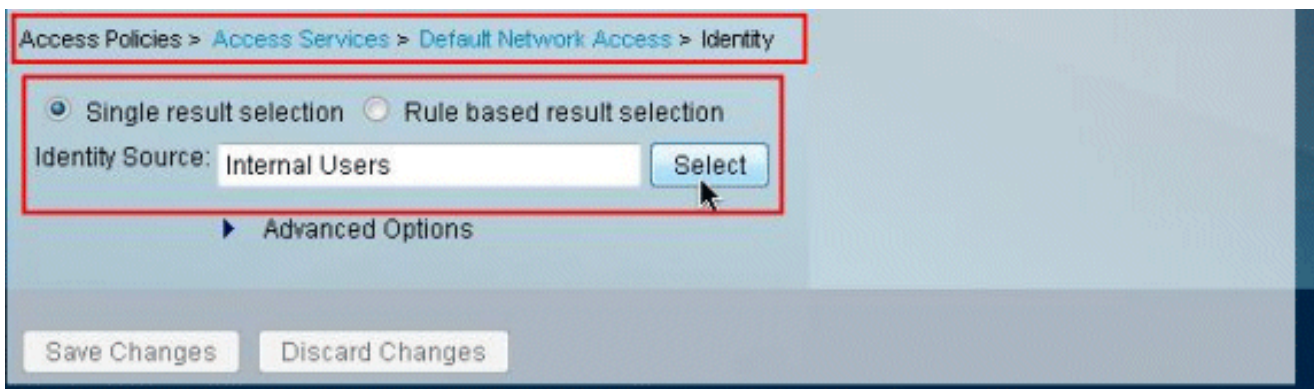
1. أختار سياسات الوصول < خدمات الوصول > قواعد تحديد الخدمة، وتحقق من الخدمة التي ستستخدم خادم LDAP للمصادقة. في هذا المثال، تستخدم مصادقة خادم LDAP خدمة الوصول إلى الشبكة الافتراضية.



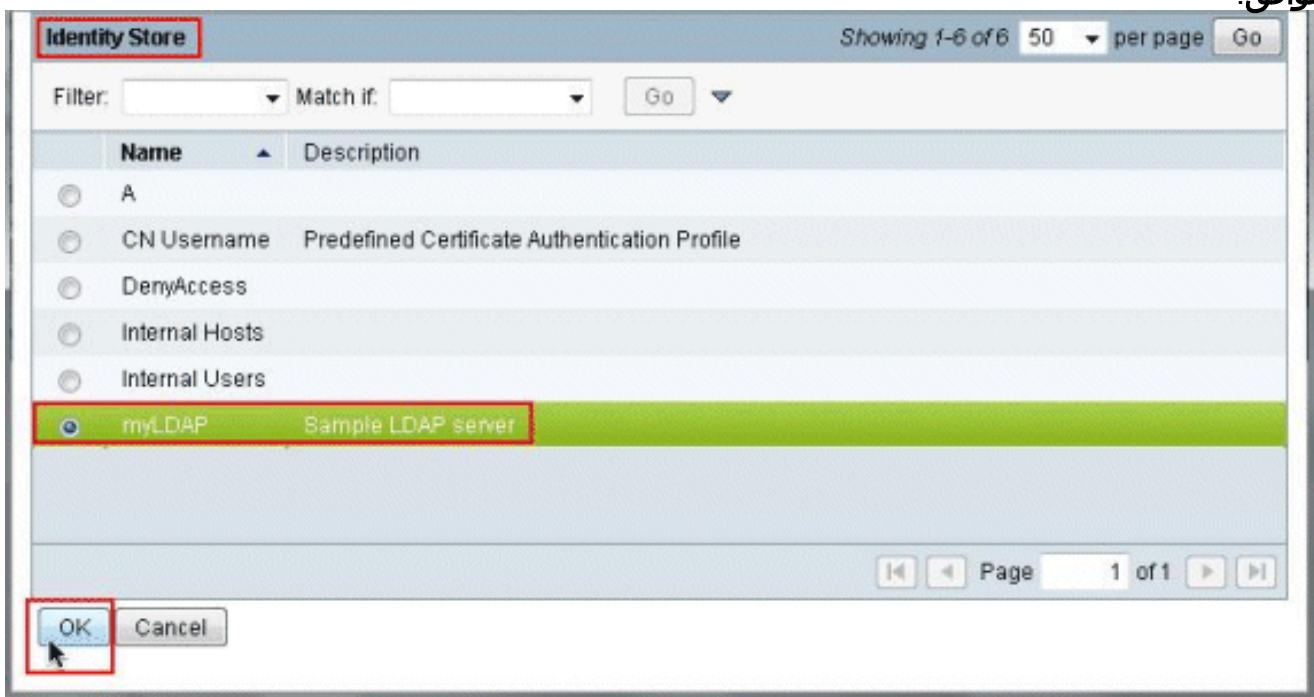
2. بمجرد التحقق من الخدمة في الخطوة 1، انتقل إلى الخدمة المحددة وانقر فوق البروتوكولات المسموح بها. تأكد من تحديد السماح ب PAP/ASCII، وانقر إرسال. ملاحظة: يمكنك تحديد بروتوكولات مصادقة أخرى مع السماح ب PAP/ASCII.



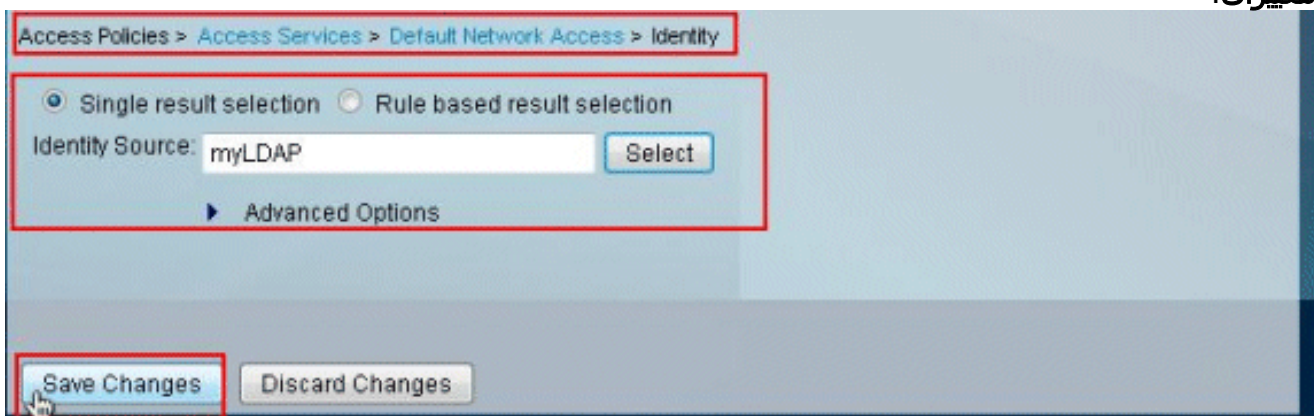
3. انقر فوق الخدمة المحددة في الخطوة 1، ثم انقر فوق الهوية. انقر فوق تحديد إلى يمين حقل مصدر الهوية.



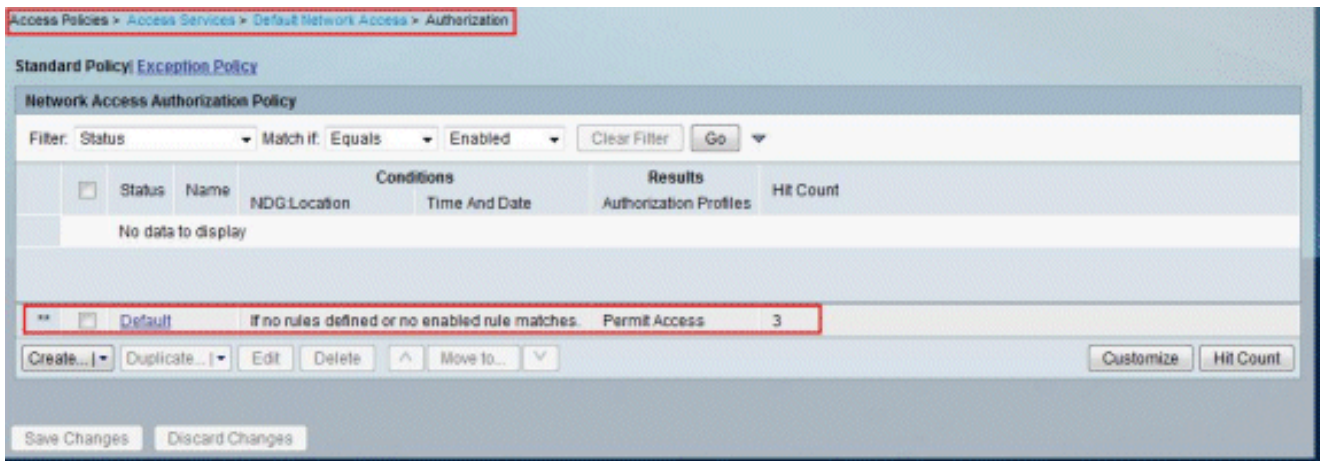
4. حدد خادم LDAP الذي تم إنشاؤه حديثاً (MyLDAP، في هذا المثال)، وانقر فوق موافق.



5. انقر فوق حفظ التغييرات.



6. انتقل إلى قسم التحويل 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 مدعوم الخادم معطلت ذاكرة الخادم المستخدم ليس لديه امتيازات تم تكوين بيانات اعتماد مسؤول غير صحيحة
 - أخطاء الربط - الأسباب المحتملة لخادم LDAP لإرجاع أخطاء الربط (المصادقة) هي: أخطاء التصفية فشل البحث باستخدام معايير المرشحات أخطاء المعلمة تم إدخال معلومات غير صحيحة حساب المستخدم مقيد (معطل، مؤمن، منتهى 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
- نفذت ذاكرة الخادم

المستخدم خطأ تم تسجيله كخطأ مستخدم غير معروف.

تم تسجيل خطأ كخطأ كلمة مرور غير صحيح، حيث يوجد المستخدم، ولكن كلمة المرور المرسله غير صحيحة.

معلومات ذات صلة

- [نظام التحكم في الوصول الآمن من Cisco](#)
- [طبائات التعليقات \(RFCs\)](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مه تلبل
Cisco يخلت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤتو تامچرتل هذه ةقدنع اهتيلوئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچنل دن تسمل