ACS 5.x: Konfigurationsbeispiel für LDAP-Server

Inhalt

Einführung

Lightweight Directory Access Protocol (LDAP) ist ein Netzwerkprotokoll zum Abfragen und Ändern von Verzeichnisdiensten, die auf TCP/IP und UDP ausgeführt werden. LDAP ist ein einfacher Mechanismus für den Zugriff auf einen x.500-basierten Verzeichnisserver. RFC 2251 definiert LDAP.

Das Cisco Secure Access Control System (ACS) 5.x kann mithilfe des LDAP-Protokolls in eine externe LDAP-Datenbank (auch als Identitätsspeicher bezeichnet) integriert werden. Es gibt zwei Methoden, um eine Verbindung zum LDAP-Server herzustellen: Klartext (einfach) und SSL (verschlüsselt) Verbindung. ACS 5.x kann für die Verbindung mit dem LDAP-Server mit beiden dieser Methoden konfiguriert werden. Dieses Dokument enthält ein Konfigurationsbeispiel für die Verbindung von ACS 5.x mit einem LDAP-Server über eine einfache Verbindung.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass der ACS 5.x über eine IP-Verbindung zum LDAP-Server verfügt und der Port TCP 389 offen ist.

Standardmäßig ist der Microsoft Active Directory-LDAP-Server so konfiguriert, dass er LDAP-Verbindungen auf dem Port TCP 389 akzeptiert. Wenn Sie einen anderen LDAP-Server verwenden, stellen Sie sicher, dass dieser aktiv ist und Verbindungen auf Port TCP 389

akzeptiert.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Secure ACS 5.x
- Microsoft Active Directory LDAP-Server

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Verzeichnisdienst

Der Verzeichnisdienst ist eine Softwareanwendung oder eine Gruppe von Anwendungen, die zum Speichern und Organisieren von Informationen über die Benutzer und Netzwerkressourcen eines Computernetzwerks verwendet wird. Sie können den Verzeichnisdienst verwenden, um den Benutzerzugriff auf diese Ressourcen zu verwalten.

Der LDAP-Verzeichnisdienst basiert auf einem Client-Server-Modell. Ein Client stellt eine Verbindung zu einem LDAP-Server her, um eine LDAP-Sitzung zu starten, und sendet betriebliche Anforderungen an den Server. Der Server sendet dann seine Antworten. Ein oder mehrere LDAP-Server enthalten Daten aus der LDAP-Verzeichnisstruktur oder der LDAP-Backend-Datenbank.

Der Verzeichnisdienst verwaltet das Verzeichnis, d. h. die Datenbank, in der die Informationen gespeichert sind. Verzeichnisdienste verwenden ein verteiltes Modell, um Informationen zu speichern, und diese Informationen werden in der Regel zwischen Verzeichnisservern repliziert.

Ein LDAP-Verzeichnis ist in einer einfachen Baumhierarchie organisiert und kann auf viele Server verteilt werden. Jeder Server kann über eine replizierte Version des Gesamtverzeichnisses verfügen, die regelmäßig synchronisiert wird.

Ein Eintrag in der Struktur enthält eine Reihe von Attributen, bei denen jedes Attribut einen Namen (einen Attributtyp oder eine Attributbeschreibung) und einen oder mehrere Werte hat. Die Attribute werden in einem Schema definiert.

Jeder Eintrag verfügt über eine eindeutige ID, die als Distinguished Name (DN) bezeichnet wird. Dieser Name enthält den RDN (Relative Distinguished Name), der aus Attributen im Eintrag erstellt wurde, gefolgt von der DN des übergeordneten Eintrags. Sie können sich den DN als vollständigen Dateinamen und den RDN als relativen Dateinamen in einem Ordner vorstellen.

Authentifizierung über LDAP

ACS 5.x kann einen Principal für einen LDAP-Identitätsspeicher authentifizieren, indem er eine Bindungsoperation auf dem Verzeichnisserver durchführt, um den Principal zu finden und zu authentifizieren. Wenn die Authentifizierung erfolgreich ist, kann der ACS Gruppen und Attribute abrufen, die dem Principal angehören. Die abzurufenden Attribute können in der ACS-Webschnittstelle (LDAP-Seiten) konfiguriert werden. Diese Gruppen und Attribute können von ACS verwendet werden, um den Principal zu autorisieren.

Um einen Benutzer zu authentifizieren oder den LDAP-Identitätsspeicher abzufragen, stellt der ACS eine Verbindung zum LDAP-Server her und verwaltet einen Verbindungspool. Siehe LDAP-Verbindungsverwaltung.

LDAP-Verbindungsmanagement

ACS 5.x unterstützt mehrere gleichzeitige LDAP-Verbindungen. Verbindungen werden bei Bedarf zum Zeitpunkt der ersten LDAP-Authentifizierung geöffnet. Die maximale Anzahl von Verbindungen wird für jeden LDAP-Server konfiguriert. Das Öffnen von Verbindungen im Voraus verkürzt die Authentifizierungszeit.

Sie können die maximale Anzahl von Verbindungen festlegen, die für gleichzeitige Bindungsverbindungen verwendet werden sollen. Die Anzahl der geöffneten Verbindungen kann für jeden LDAP-Server (primär oder sekundär) unterschiedlich sein und wird anhand der maximalen Anzahl der für jeden Server konfigurierten Administrationsverbindungen bestimmt.

ACS behält eine Liste offener LDAP-Verbindungen (einschließlich der binden Informationen) für jeden LDAP-Server bei, der in ACS konfiguriert ist. Während des Authentifizierungsprozesses versucht der Verbindungs-Manager, eine offene Verbindung aus dem Pool zu finden.

Wenn keine offene Verbindung vorhanden ist, wird eine neue geöffnet. Wenn der LDAP-Server die Verbindung geschlossen hat, meldet der Verbindungs-Manager beim ersten Aufruf zum Durchsuchen des Verzeichnisses einen Fehler und versucht, die Verbindung zu erneuern.

Wenn der Authentifizierungsprozess abgeschlossen ist, gibt der Connection Manager die Verbindung zum Connection Manager frei. Weitere Informationen finden Sie im ACS 5.X-Benutzerhandbuch.

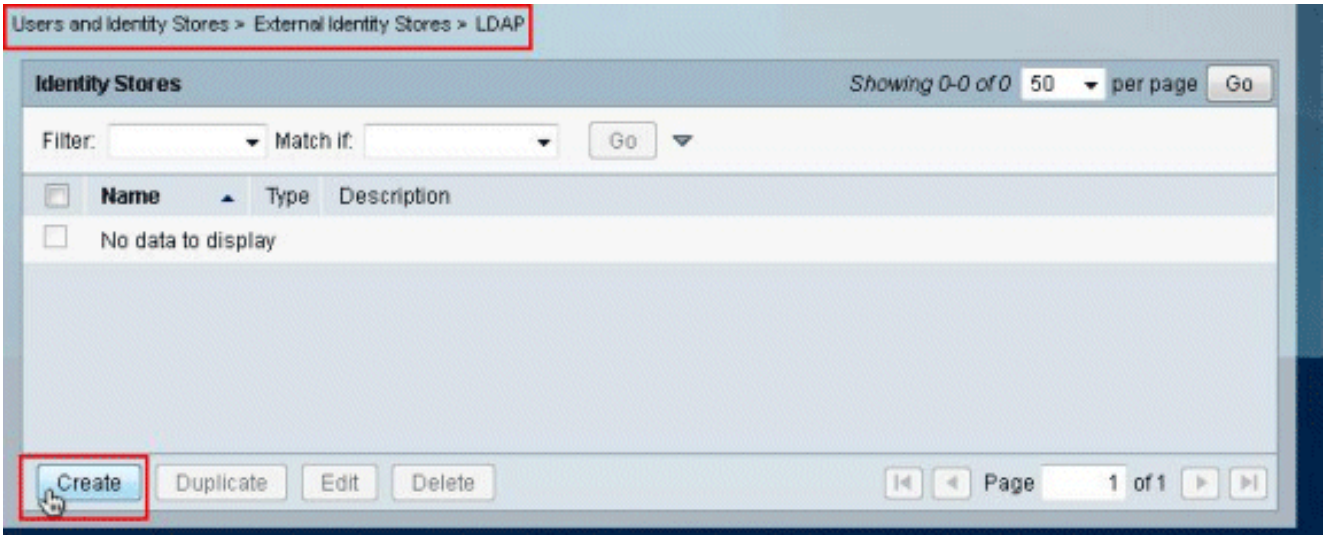
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

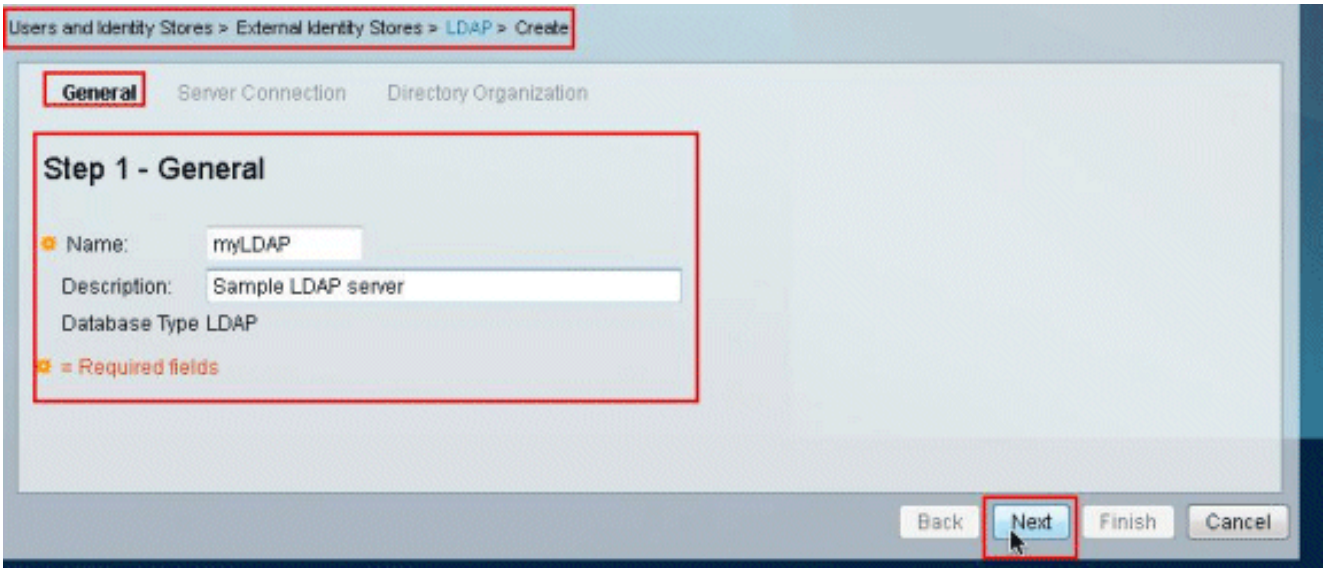
Konfigurieren von ACS 5.x für LDAP

Gehen Sie wie folgt vor, um ACS 5.x für LDAP zu konfigurieren:

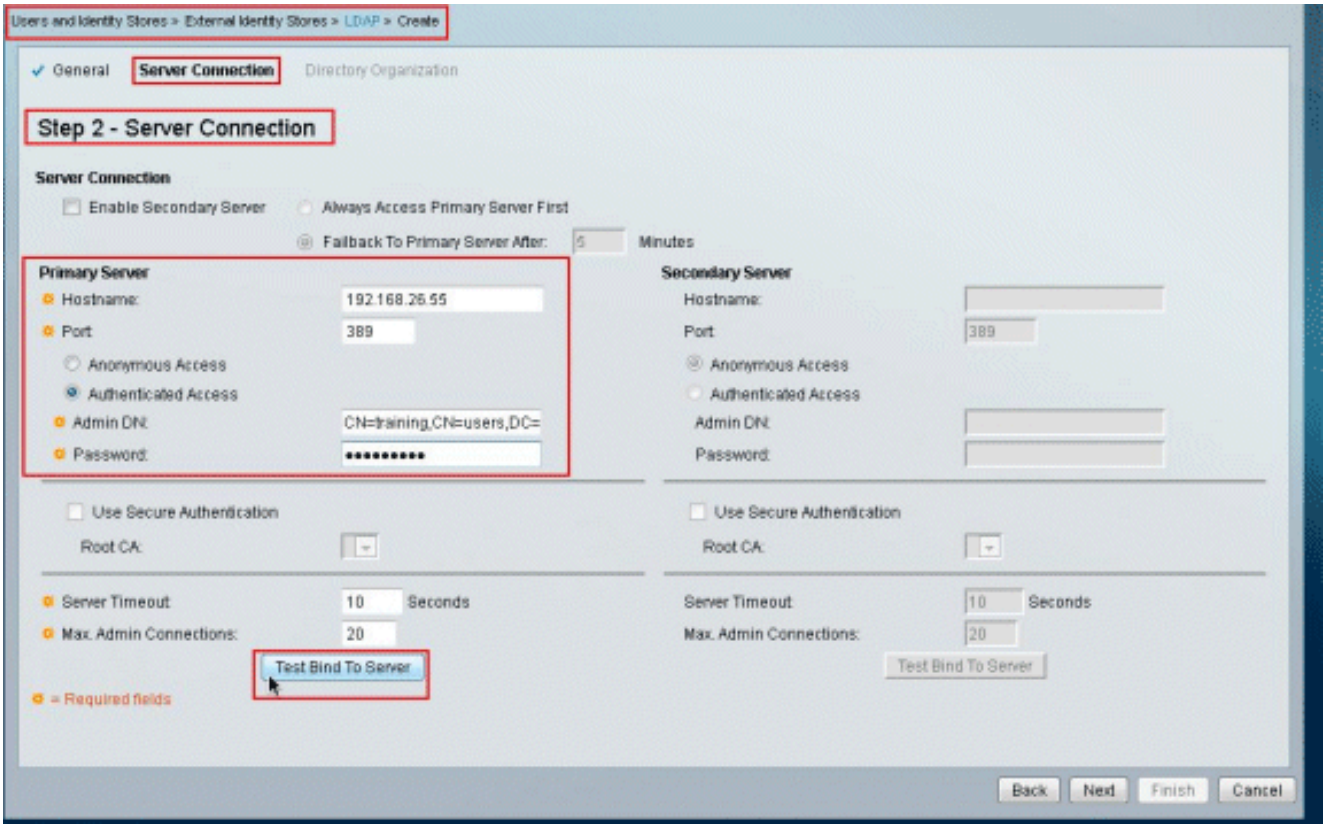
1. Wählen Sie **Benutzer und Identitätsdatenbanken > Externe Identitätsdatenbanken > LDAP**, und klicken Sie auf **Erstellen**, um eine neue LDAP-Verbindung zu erstellen.



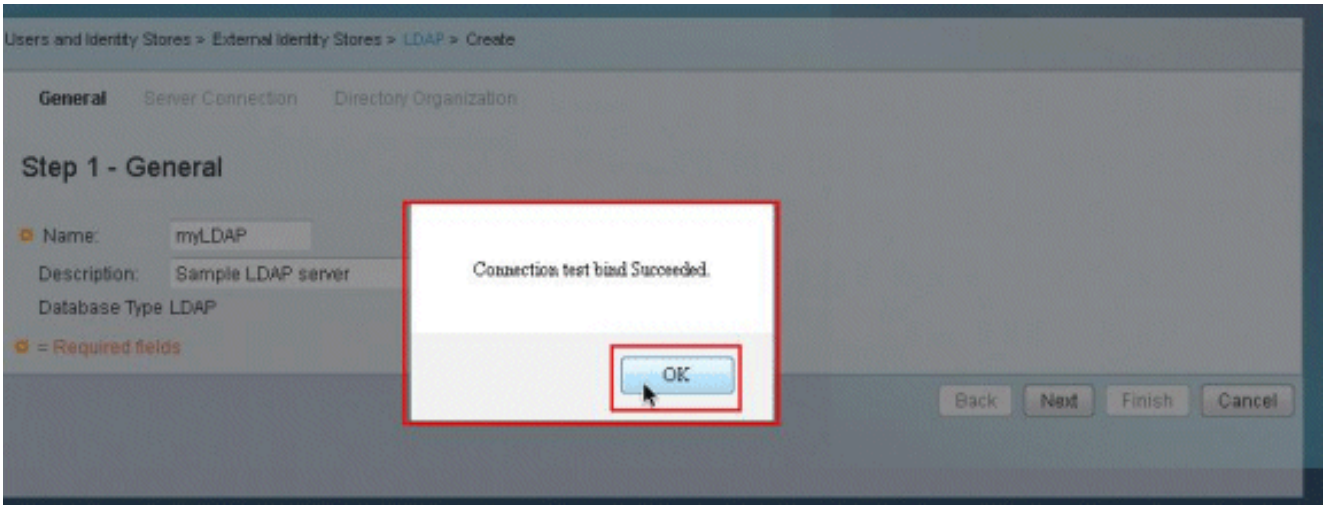
2. Geben Sie auf der Registerkarte Allgemein den **Namen** und die **Beschreibung** (optional) für das neue LDAP an, und klicken Sie auf **Weiter**.



3. Geben Sie auf der Registerkarte "Serververbindung" im Abschnitt "Primärer Server" den **Hostnamen**, den **Port**, die **Admin-DN** und das **Kennwort ein**. Klicken Sie auf **Testbindung an Server**.**Hinweis:** Die IANA-zugewiesene Portnummer für LDAP ist TCP 389. Bestätigen Sie jedoch die Portnummer, die Ihr LDAP-Server verwendet, vom LDAP-Administrator. Die Admin-DN und das Passwort sollten Ihnen vom LDAP-Administrator bereitgestellt werden. Ihre Admin-DN muss über alle Berechtigungen für alle OUs auf dem LDAP-Server verfügen.

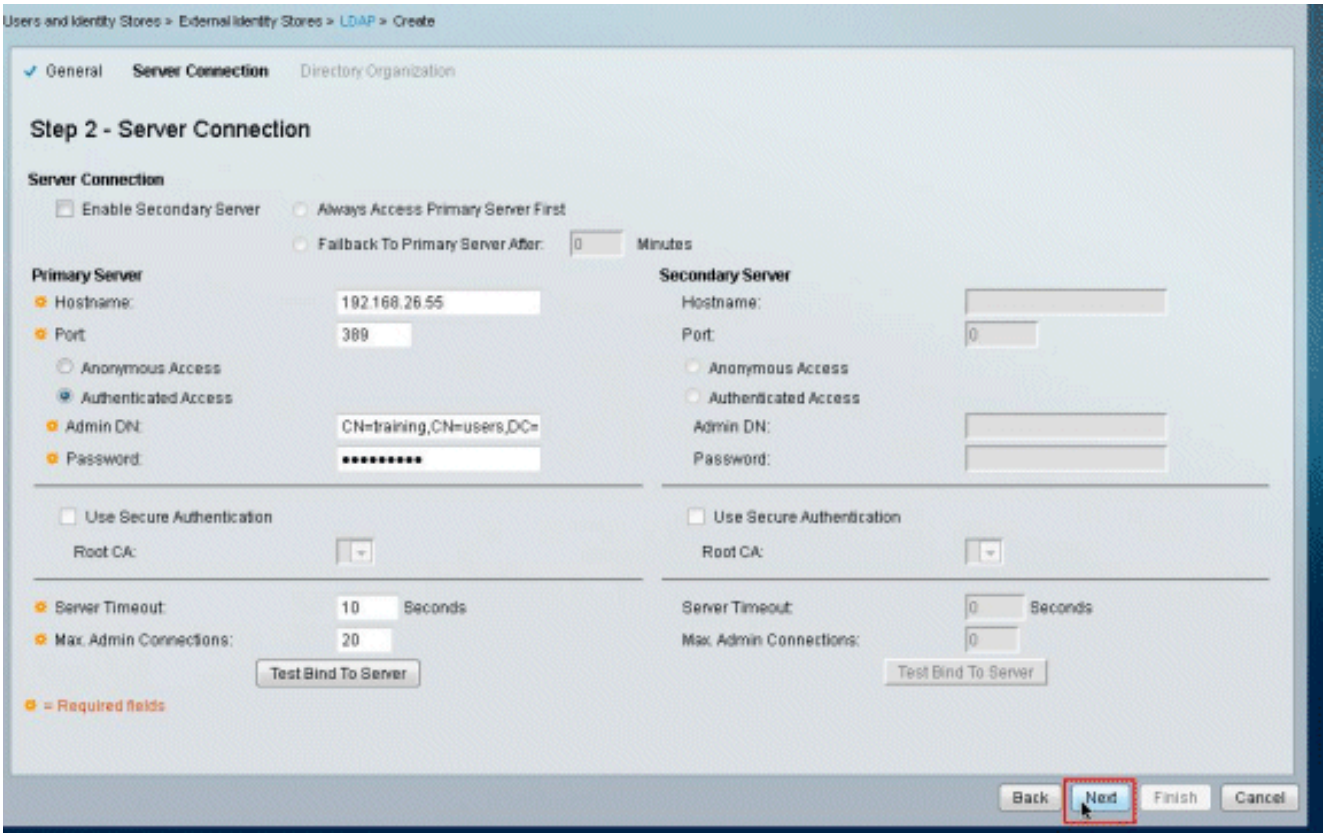


4. Dieses Bild zeigt, dass das **Verbindungstestbind zum Server** erfolgreich war.

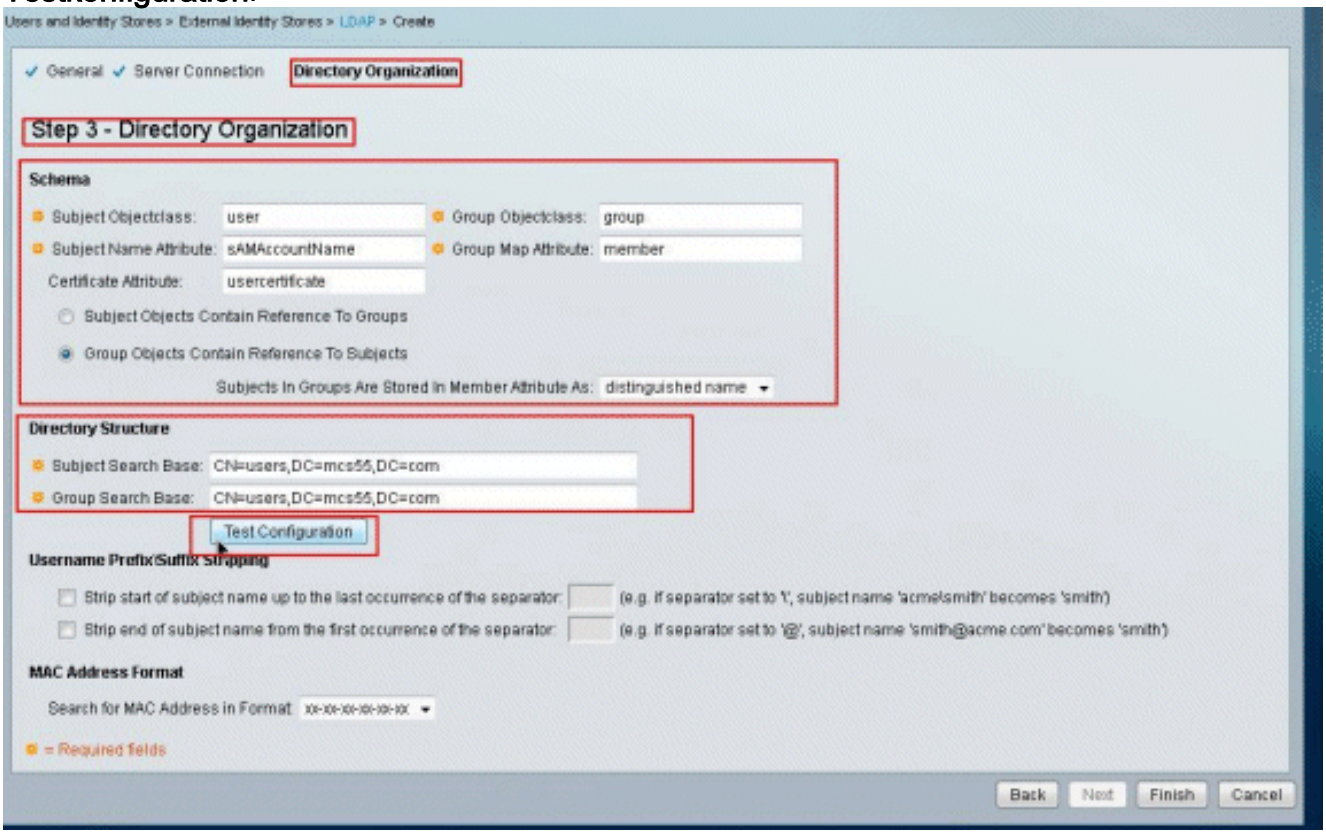


Hinweis: Wenn die Testbindung nicht erfolgreich ist, überprüfen Sie den **Hostnamen**, die **Portnummer**, die **Admin-DN** und das **Passwort** Ihres LDAP-Administrators.

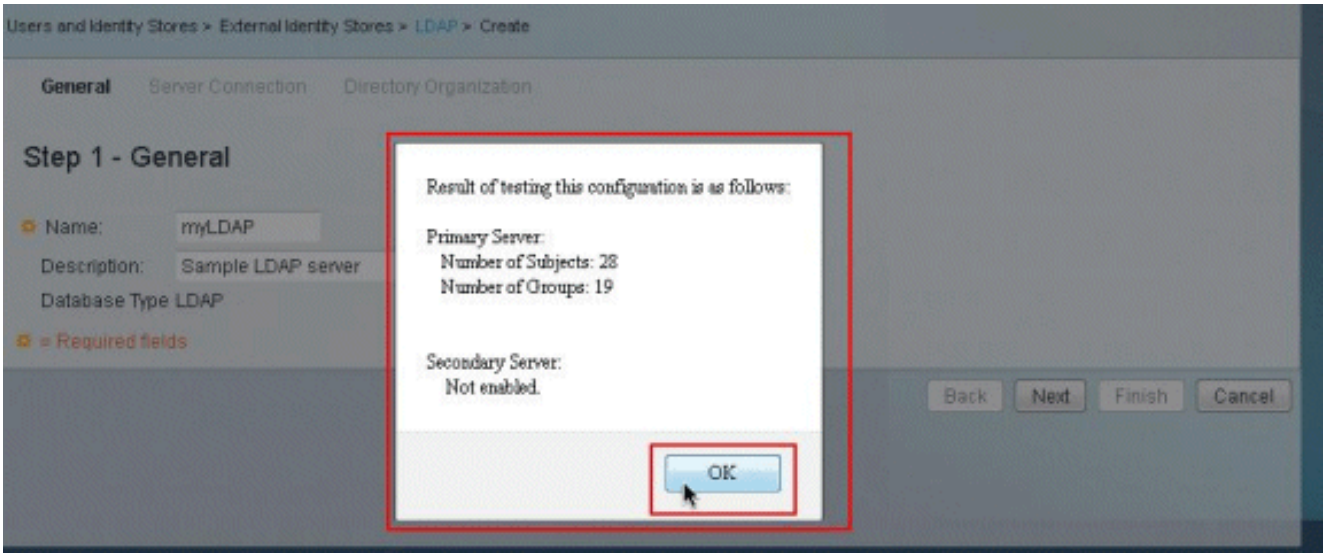
5. Klicken Sie auf **Weiter**.



6. Geben Sie auf der Registerkarte Verzeichnisorganisation im Abschnitt Schema die erforderlichen Details ein. Geben Sie entsprechend die erforderlichen Informationen im Bereich Verzeichnisstruktur an, wie vom LDAP-Administrator bereitgestellt. Klicken Sie auf **Testkonfiguration**.

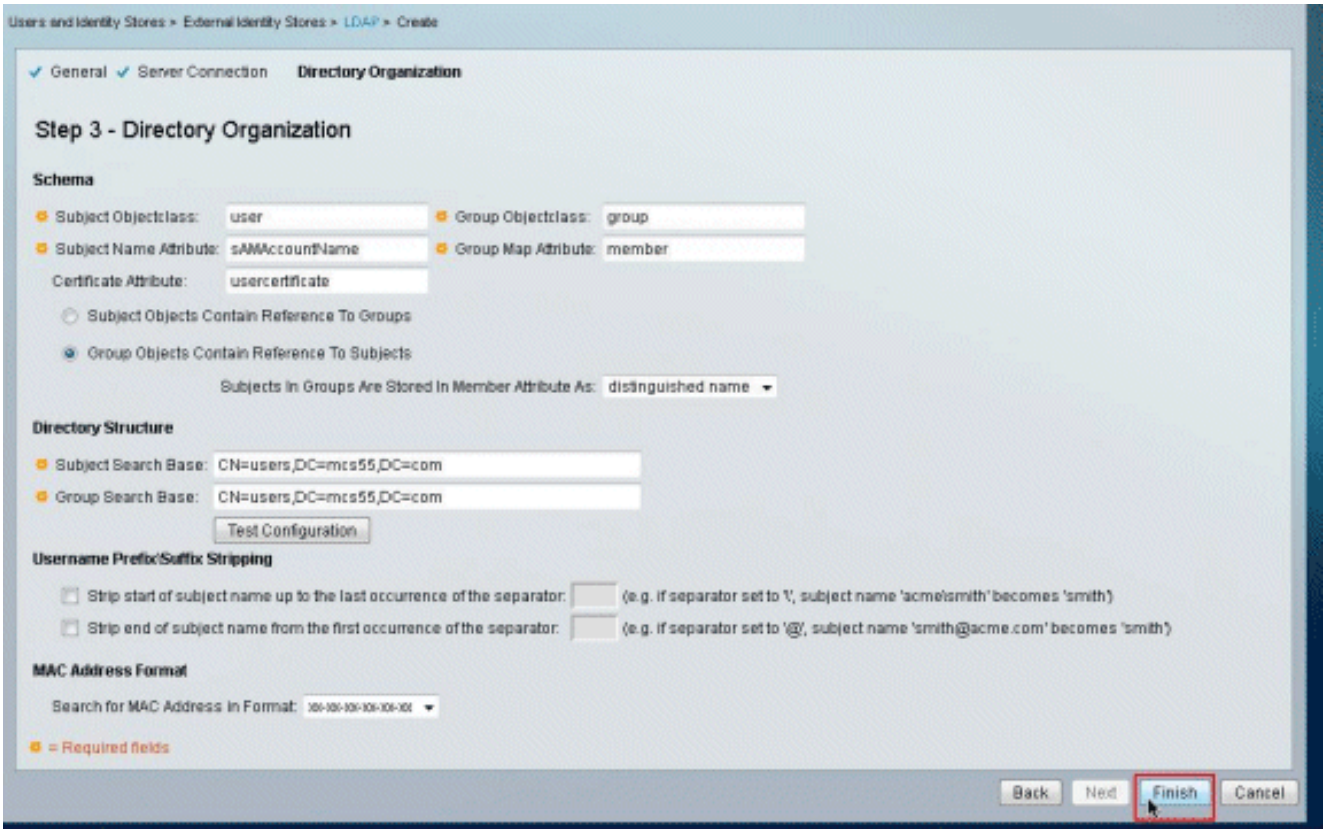


7. Dieses Bild zeigt, dass der **Konfigurationstest** erfolgreich durchgeführt wurde.

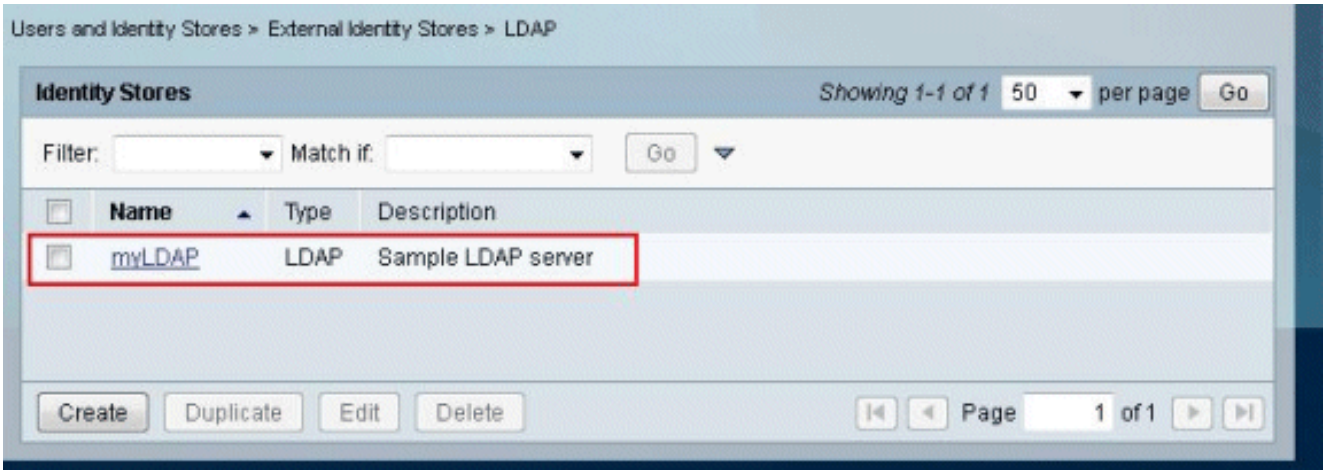


Hinweis: Wenn der Konfigurationstest nicht erfolgreich ist, überprüfen Sie die Parameter im **Schema** und in der **Verzeichnisstruktur** erneut von Ihrem LDAP-Administrator.

8. Klicken Sie auf **Fertig stellen**.

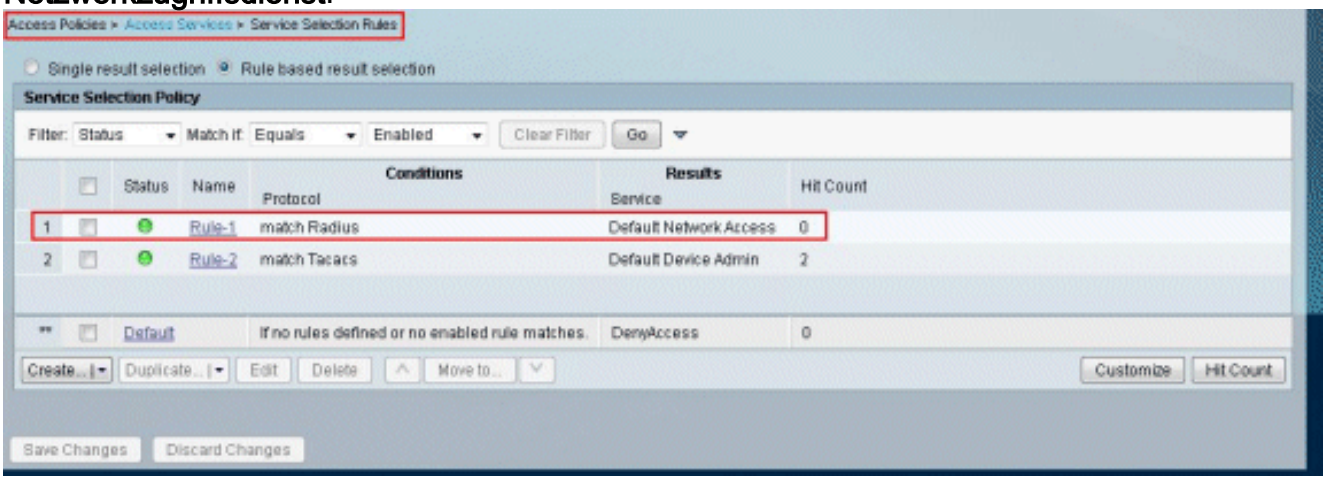


9. Der **LDAP-Server** wurde erfolgreich erstellt.

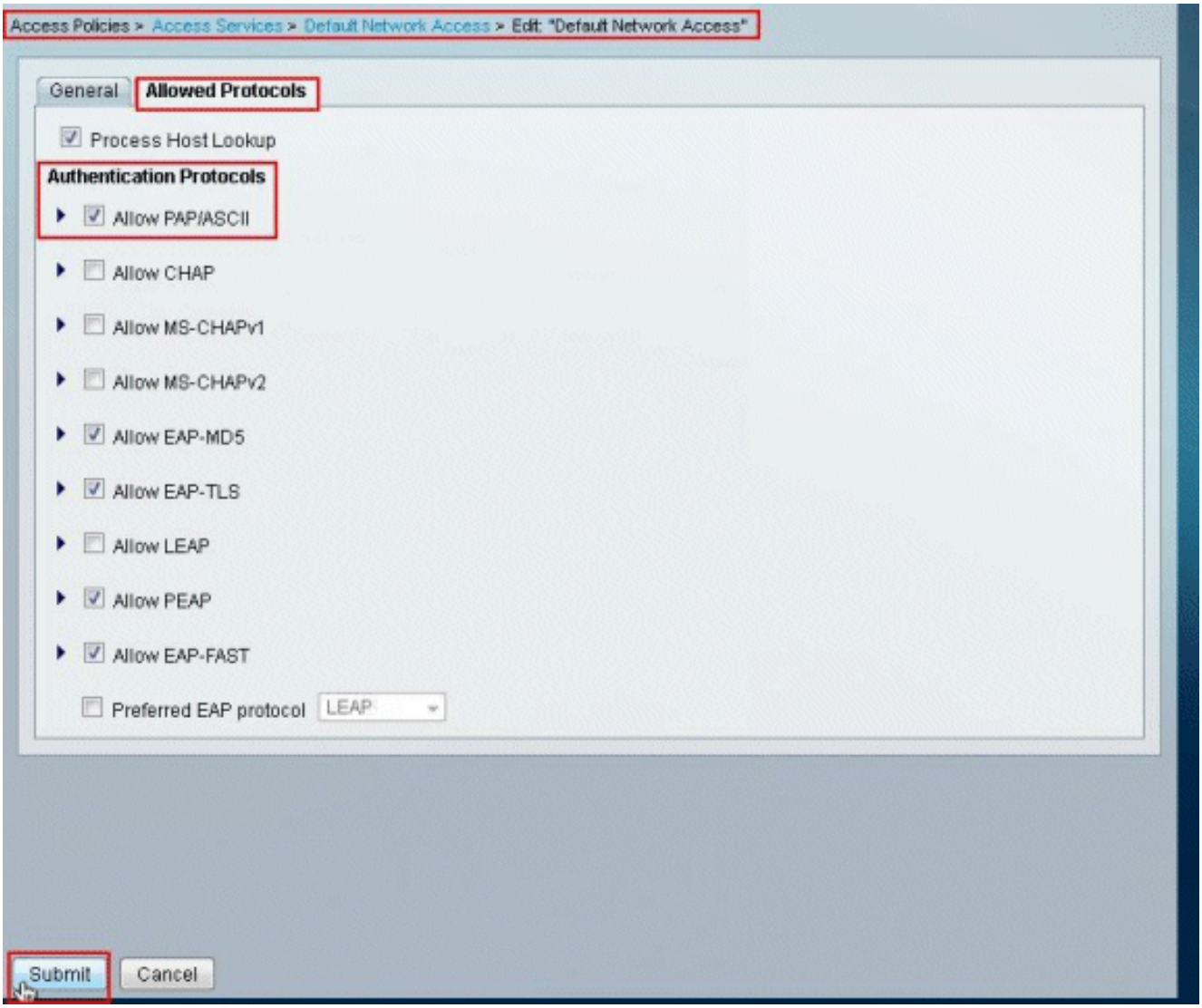


Konfigurieren des Identitätsspeichers

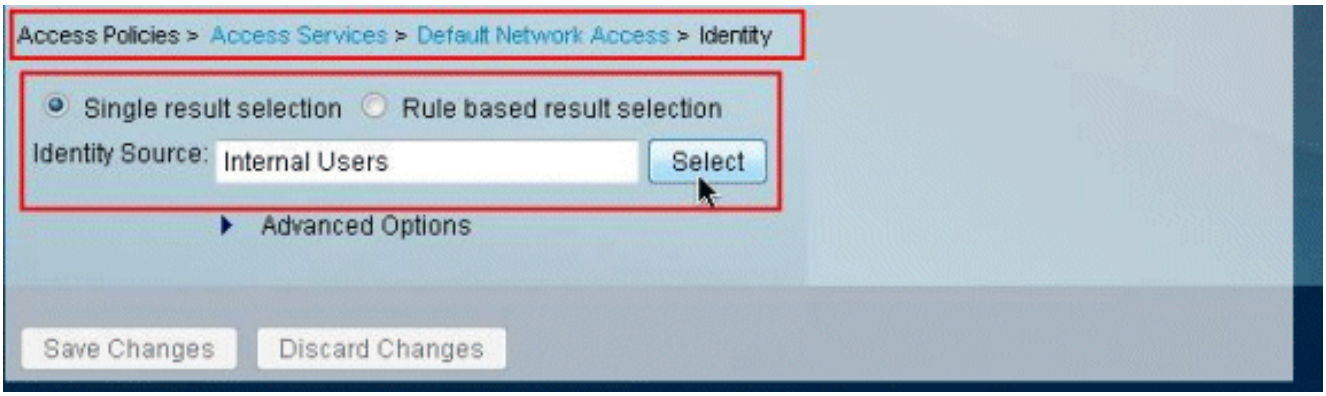
Gehen Sie wie folgt vor, um den Identity Store zu konfigurieren:

1. Wählen Sie **Zugriffsrichtlinien > Zugriffsdienste > Service Selection Rules (Dienstauswahlregeln) aus**, und überprüfen Sie, welcher Dienst den LDAP-Server für die Authentifizierung verwendet. In diesem Beispiel verwendet die LDAP-Serverauthentifizierung den **Standard-Netzwerkzugriffsdienst**.


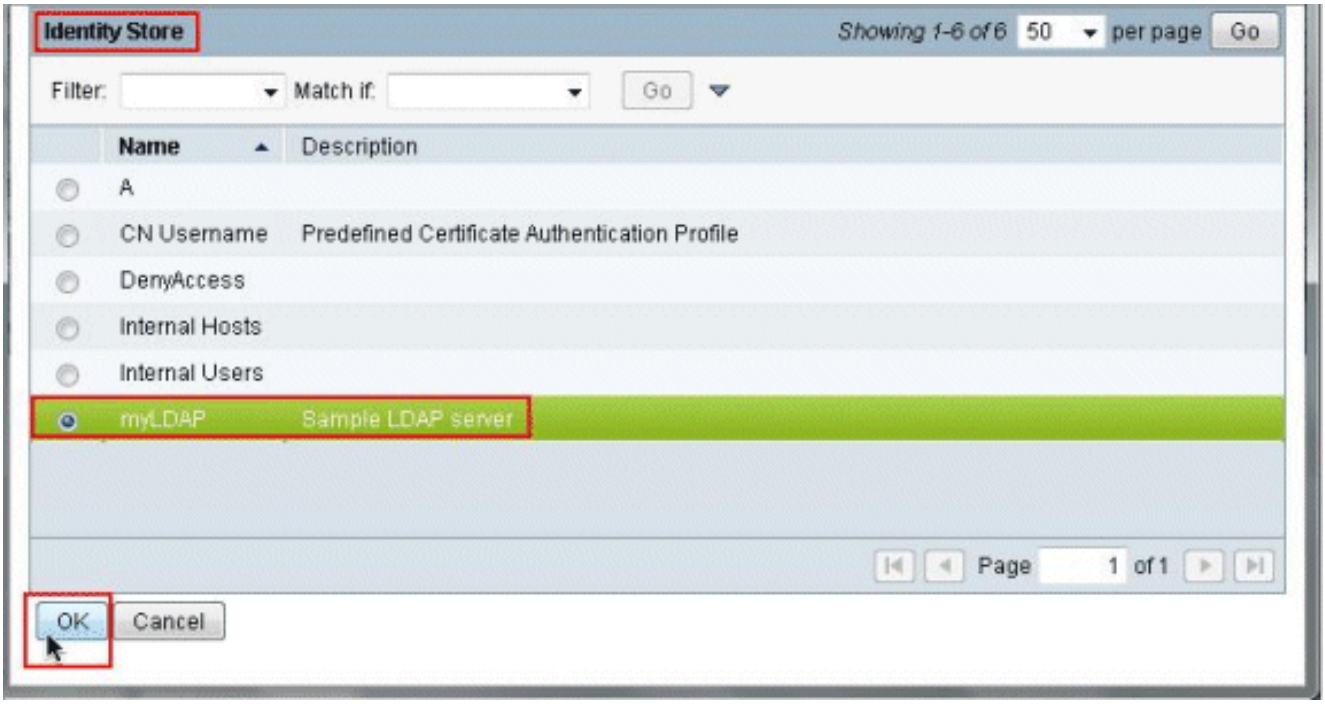
2. Sobald Sie den Service in Schritt 1 überprüft haben, gehen Sie zum jeweiligen Dienst, und klicken Sie auf **Zulässige Protokolle**. Vergewissern Sie sich, dass **PAP/ASCII zulassen** aktiviert ist, und klicken Sie auf **Senden**.**Hinweis:** Sie können andere Authentifizierungsprotokolle zusammen mit PAP/ASCII zulassen auswählen.



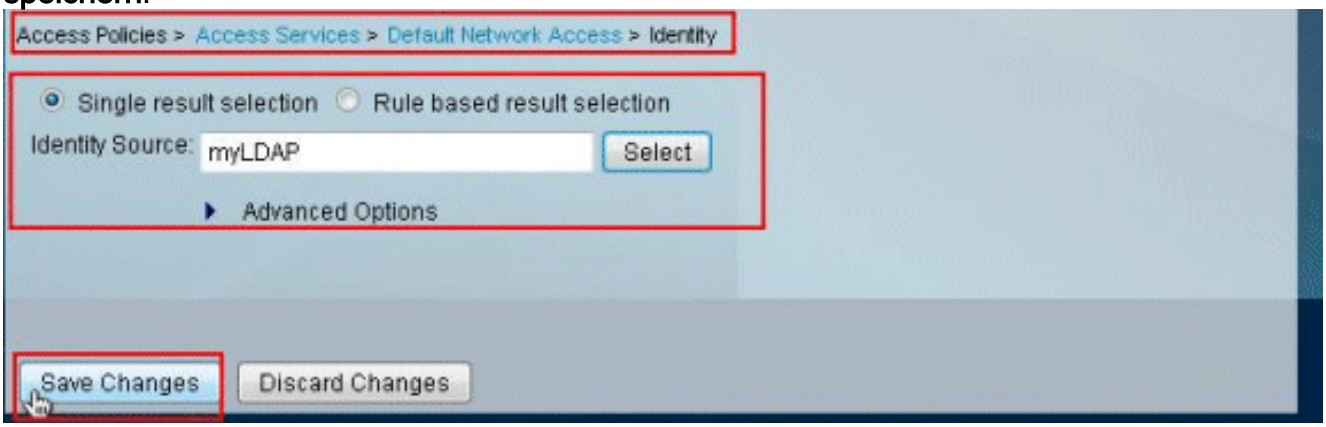
3. Klicken Sie auf den in Schritt 1 identifizierten Service und anschließend auf **Identität**. Klicken Sie rechts neben dem Feld Identitätsquelle auf **Auswählen**.



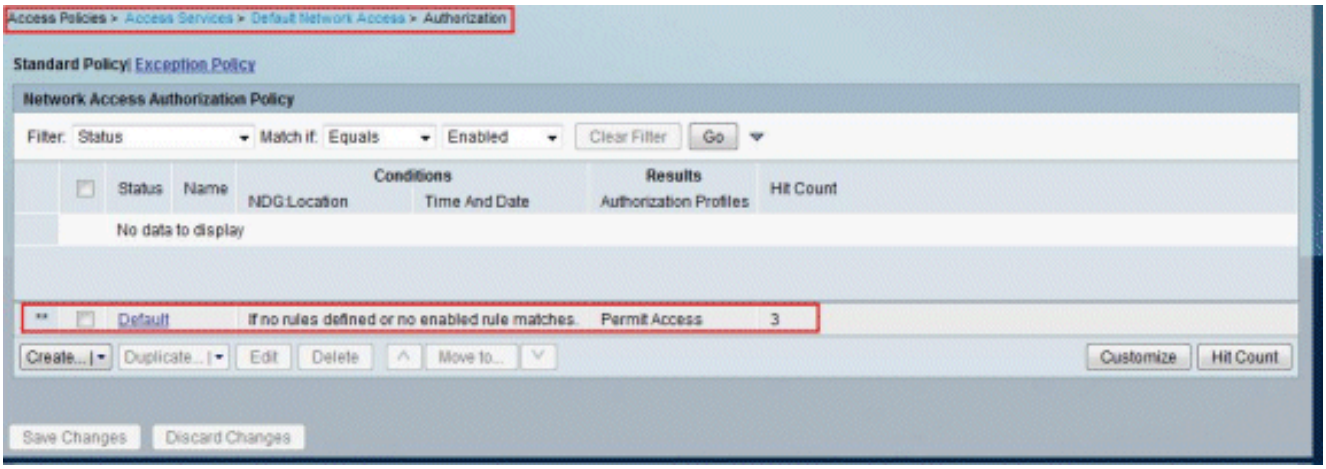
4. Wählen Sie den neu erstellten LDAP-Server (in diesem Beispiel **myLDAP**) aus, und klicken Sie auf **OK**.



5. Klicken Sie auf **Änderungen speichern**.



6. Gehen Sie zum Abschnitt Autorisierung des in Schritt 1 identifizierten Dienstes, und stellen Sie sicher, dass mindestens eine Regel für die **Authentifizierung** vorhanden ist.



Fehlerbehebung

ACS sendet eine Verbindungsanforderung, um den Benutzer gegen einen LDAP-Server zu authentifizieren. Die Bindungsanforderung enthält die DN und das Benutzerkennwort des

Benutzers in Klartext. Ein Benutzer wird authentifiziert, wenn die DN und das Kennwort des Benutzers mit dem Benutzernamen und Kennwort im LDAP-Verzeichnis übereinstimmen.

- **Authentifizierungsfehler** - ACS protokolliert Authentifizierungsfehler in den ACS-Protokolldateien.
- **Initialisierungsfehler** - Verwenden Sie die Zeitüberschreitungseinstellungen des LDAP-Servers, um die Anzahl der Sekunden zu konfigurieren, die der ACS auf eine Antwort von einem LDAP-Server wartet, bevor festgestellt wird, dass die Verbindung oder Authentifizierung auf diesem Server fehlgeschlagen ist. Mögliche Gründe, warum ein LDAP-Server einen Initialisierungsfehler zurückgibt, sind:LDAP wird nicht unterstütztDer Server ist ausgefallen.Der Server ist nicht ausgelastet.Der Benutzer hat keine Berechtigungen.Falsche Administratoranmeldeinformationen werden konfiguriert.
- **Bind-Fehler** - Möglicherweise gibt ein LDAP-Server Bind-Fehler (Authentifizierung) zurück:FilterfehlerEine Suche mithilfe von Filterkriterien schlägt fehlParameterfehlerUngültige Parameter wurden eingegeben.Das Benutzerkonto ist eingeschränkt (deaktiviert, gesperrt, abgelaufen, Kennwort abgelaufen usw.)

Diese Fehler werden als externe Ressourcenfehler protokolliert, was auf ein mögliches Problem mit dem LDAP-Server hinweist:

- Es ist ein Verbindungsfehler aufgetreten
- Das Timeout ist abgelaufen
- Der Server ist ausgefallen.
- Der Server ist nicht ausgelastet.

Der Fehler `Ein Benutzer ist nicht in der Datenbank vorhanden` wird als Fehler Unbekannter Benutzer protokolliert.

Der Fehler `Ein ungültiges Kennwort wurde eingegeben` wird als Fehler mit ungültigem Kennwort protokolliert, wenn der Benutzer vorhanden ist, das gesendete Kennwort jedoch ungültig ist.

Zugehörige Informationen

- Cisco Secure Access Control System
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems