ACS 5.x: Configuratievoorbeeld van LDAP-server

Inhoud

Inleiding

Lichtgewicht Directory Access Protocol (LDAP) is een netwerkprotocol voor het vragen en wijzigen van directory services die draaien op TCP/IP en UDP. LDAP is een lichtgewicht mechanisme om toegang te krijgen tot een x.500-gebaseerde folder server. RFC 2251 definieert LDAP.

Cisco Secure Access Control System (ACS) 5.x wordt geïntegreerd met een LDAP-externe database (ook wel een identiteitsopslag genoemd) met behulp van het LDAP-protocol. Er worden twee methoden gebruikt om verbinding te maken met de LDAP server: verbinding met onbewerkte tekst (eenvoudig) en SSL (versleuteld). ACS 5.x kan worden ingesteld om met beide methoden verbinding te maken met de LDAP-server. Dit document biedt een configuratievoorbeeld voor het aansluiten van ACS 5.x op een LDAP-server door middel van een eenvoudige verbinding.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat ACS 5.x een IP-verbinding heeft met de LDAP-server en dat TCP 389-poort is geopend.

Standaard wordt de Microsoft Active Directory LDAP server ingesteld om LDAP verbindingen te accepteren op poort TCP 389. Als u een andere LDAP server gebruikt, zorg er dan voor dat deze

actief is en dat er verbindingen worden geaccepteerd op poort TCP 389.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

Map-service

De telefoongids service is een softwaretoepassing of een reeks toepassingen die gebruikt worden om informatie op te slaan en te organiseren over de gebruikers en netwerkbronnen van een computernetwerk. U kunt de telefoongids service gebruiken om de toegang van gebruikers tot deze bronnen te beheren.

De LDAP-telefoongids service is gebaseerd op een clientservermodel. Een client sluit zich aan op een LDAP-server om een LDAP-sessie te starten en stuurt verzoeken om een handeling naar de server. De server stuurt dan zijn antwoorden. Een of meer LDAP-servers bevatten gegevens uit de LDAP-directory boom of de LDAP-backend-database.

De telefoongids service beheert de folder, de database die de informatie bevat. Indexdiensten gebruiken een gedistribueerd model om informatie op te slaan, en die informatie wordt gewoonlijk tussen directory servers herhaald.

Een LDAP-directory wordt georganiseerd in een eenvoudige boomstructuur en kan worden verspreid over vele servers. Elke server kan een herhaalde versie van de totale folder hebben die periodiek gesynchroniseerd wordt.

Een vermelding in de boom bevat een reeks eigenschappen, waarbij elke eigenschap een naam (een soort eigenschap of beschrijving van de eigenschap) en een of meer waarden heeft. De eigenschappen worden gedefinieerd in een schema.

Elke vermelding heeft een unieke identificator, d.w.z. de onderscheidde naam (DN). Deze naam bevat de Relative Distributed Name (RDN) geconstrueerd op basis van eigenschappen in de ingang, gevolgd door DNA van de ouderingang. Je kunt de DNA als een volledige bestandsnaam zien, en de RDN als een relatieve bestandsnaam in een map.

Verificatie met LDAP

ACS 5.x kan een aangever tegen een LDAP-identiteitsopslag authentificeren door een bindingsoperatie op de folder server uit te voeren om de aangever te vinden en te authentiseren. Als de authenticatie slaagt, kan ACS groepen en eigenschappen terugkrijgen die tot het hoofd behoren. De te herstellen eigenschappen kunnen worden ingesteld in de ACS-web interface (LDAP-pagina's). Deze groepen en eigenschappen kunnen door ACS worden gebruikt om de opdrachtgever te machtigen.

Om een gebruiker te authentiseren of het LDAP-identiteitsarchief te bevragen, sluit ACS zich aan op de LDAP-server en onderhoudt een verbindingspool. Zie LDAP-verbindingsbeheer.

LDAP-verbindingsbeheer

ACS 5.x ondersteunt meerdere parallelle LDAP-verbindingen. Aansluitingen worden op verzoek geopend op het tijdstip van de eerste authenticatie van de LDAP. Het maximale aantal verbindingen wordt ingesteld voor elke LBP-server. Het vooraf openen van verbindingen verkort de authenticatietijd.

U kunt het maximale aantal verbindingen instellen die gebruikt moeten worden voor gelijktijdige bindingsverbindingen. Het aantal geopende verbindingen kan per LDAP-server (primair of secundair) verschillend zijn en wordt bepaald op basis van het maximale aantal beheerverbindingen dat voor elke server is ingesteld.

ACS behoudt een lijst van open LDAP-verbindingen (met inbegrip van de bindingsinformatie) voor elke LDAP-server die is ingesteld in ACS. Tijdens het authenticatieproces probeert de verbindingsmanager een open verbinding uit de pool te vinden.

Als er geen open verbinding bestaat, wordt er een nieuwe geopend. Als de LDAP server de verbinding heeft gesloten, meldt de verbindingsmanager een fout tijdens de eerste aanroep om de folder te doorzoeken en probeert de verbinding te vernieuwen.

Nadat het verificatieproces is voltooid, heft de verbindingsmanager de verbinding op aan de verbindingsmanager. Raadpleeg voor meer informatie de ACS 5.X gebruikersgids.

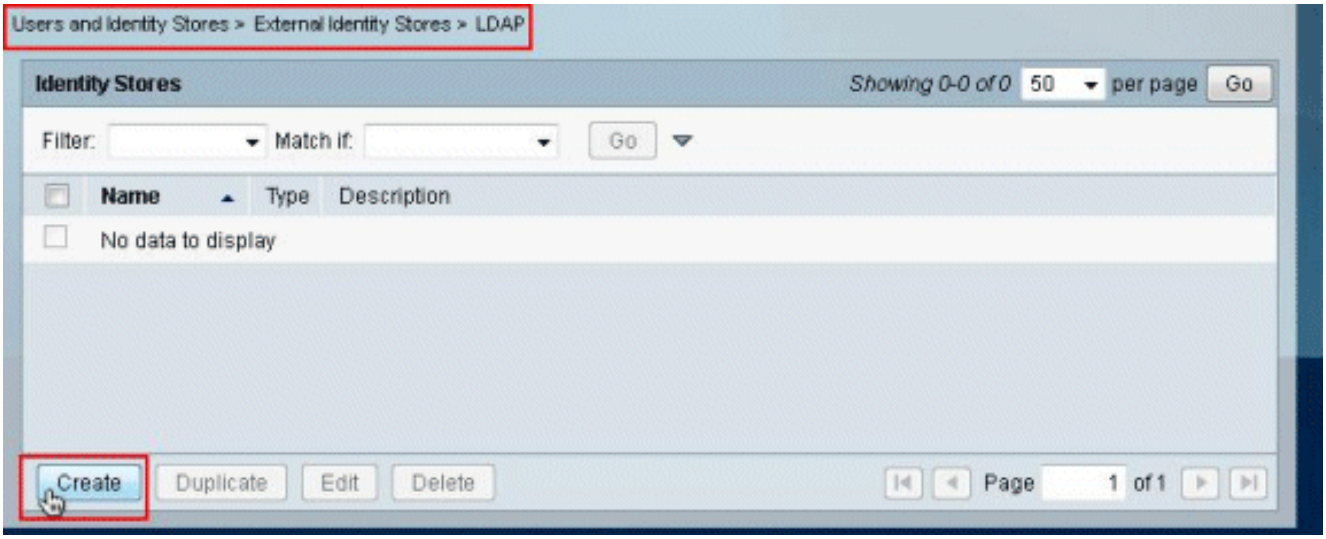
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

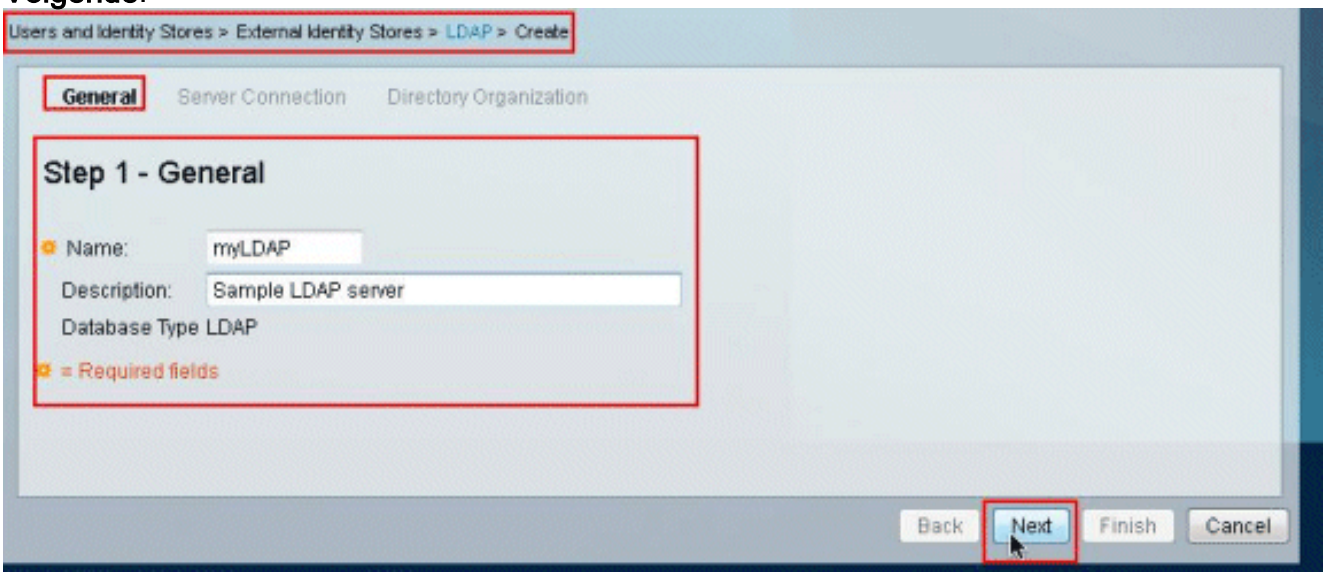
ACS 5.x configureren voor LDAP

Voltooi deze stappen om ACS 5.x voor LDAP te configureren:

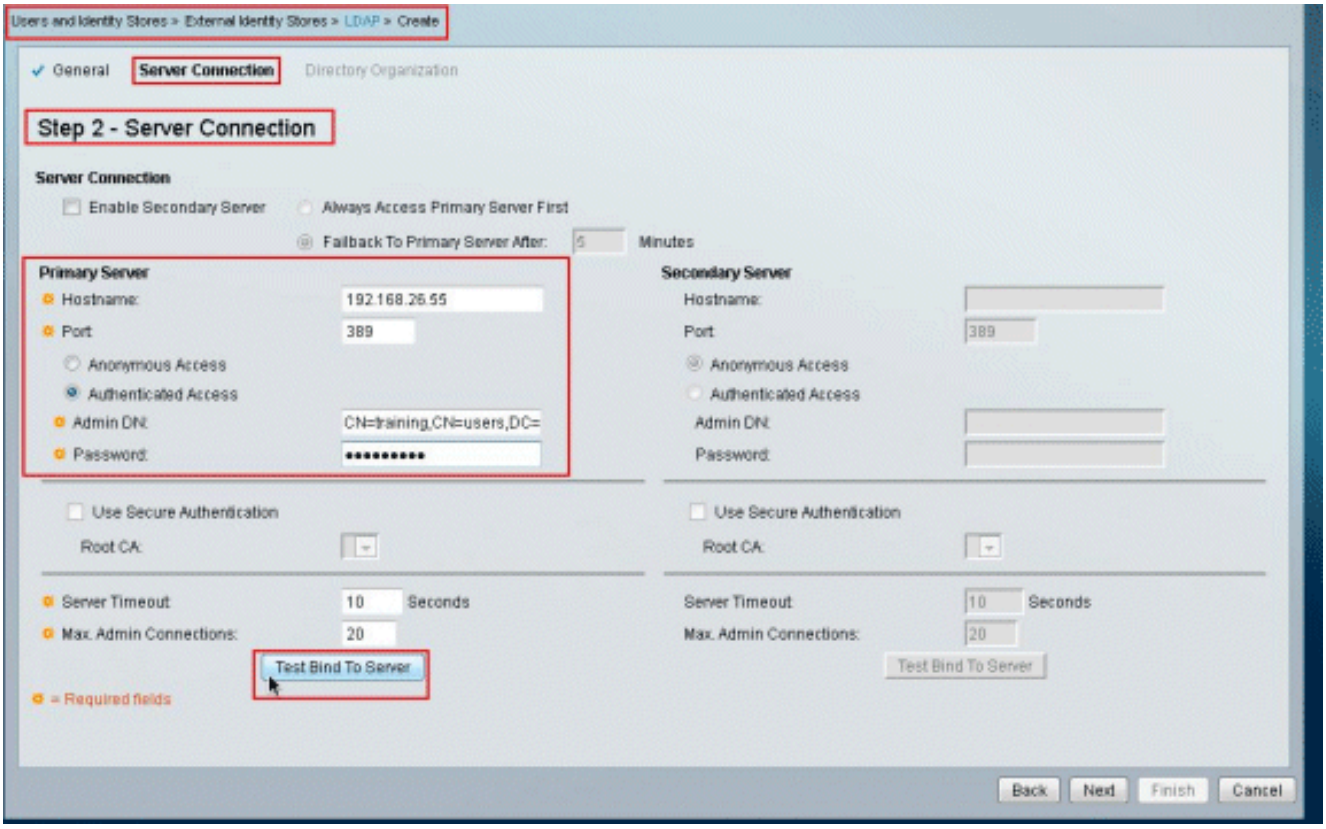
1. Kies **gebruikers en identiteitsopslag** > **Externe identiteitsopslag** > **LDAP** en klik **op Maken** om een nieuwe LDAP-verbinding te maken.



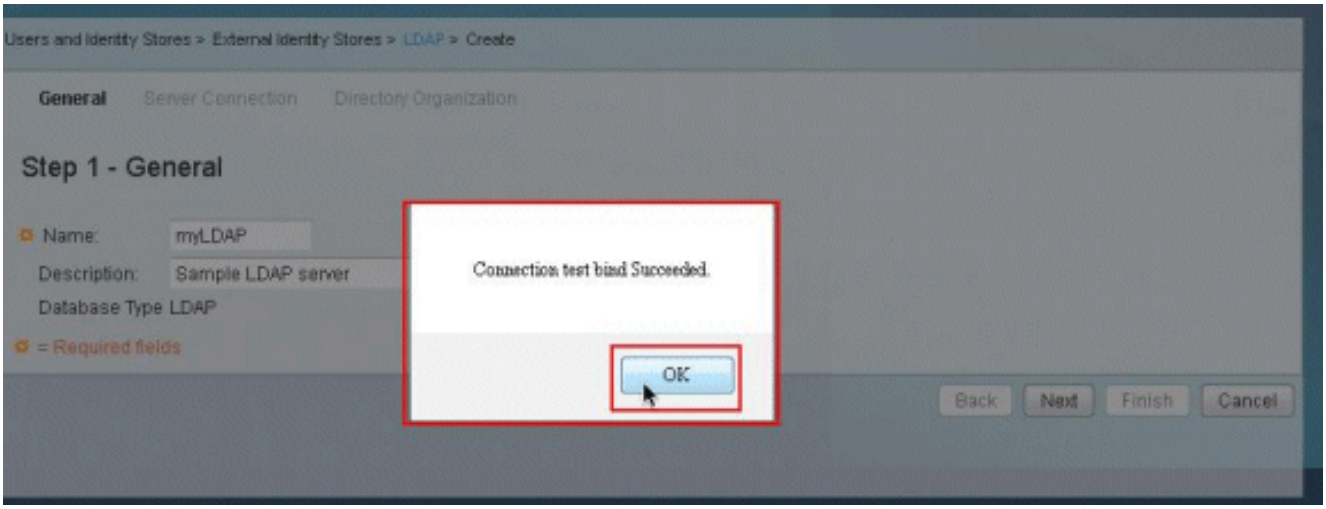
2. Typ in het tabblad Algemeen de **naam** en **omschrijving** (optioneel) voor de nieuwe LDAP en klik op
Volgende.



3. Typ in het tabblad serververbinding onder het gedeelte Primaire server de **naam** van het **ziekenhuis**, **poort**, **Admin DN** en **wachtwoord**. Klik op **Test Bind to Server**.**Opmerking:** het IANA-nummer dat aan LDAP is toegewezen, is TCP 389. Bevestig echter het poortnummer dat uw LDAP-server gebruikt vanuit uw LDAP-beheerder. Het Admin en Wachtwoord dienen aan u te worden verstrekt door uw LDAP Admin. Uw Admin DN moet alle rechten op alle OU's op de server hebben
gelezen.

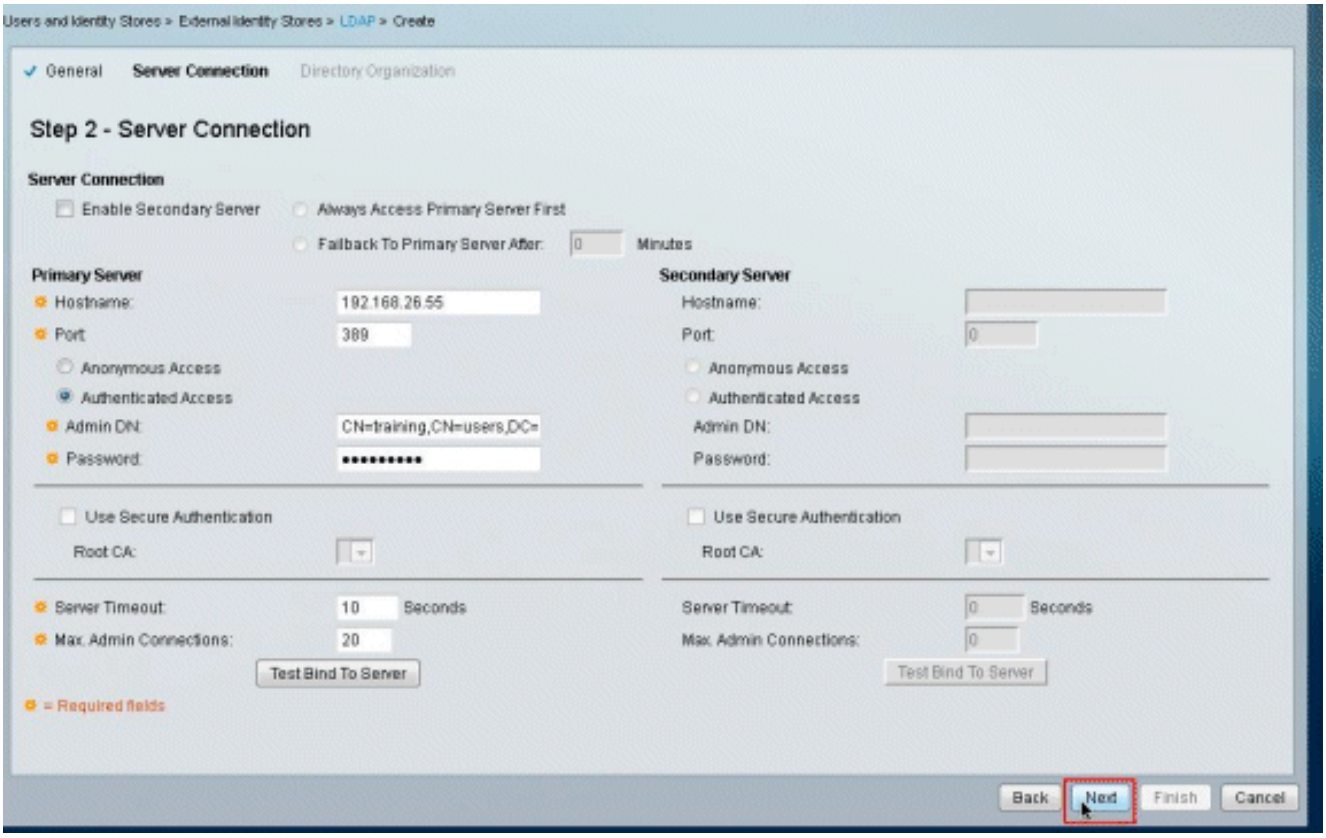


4. Deze afbeelding laat zien dat de **Connection Test Bind naar de server** geslaagd is.

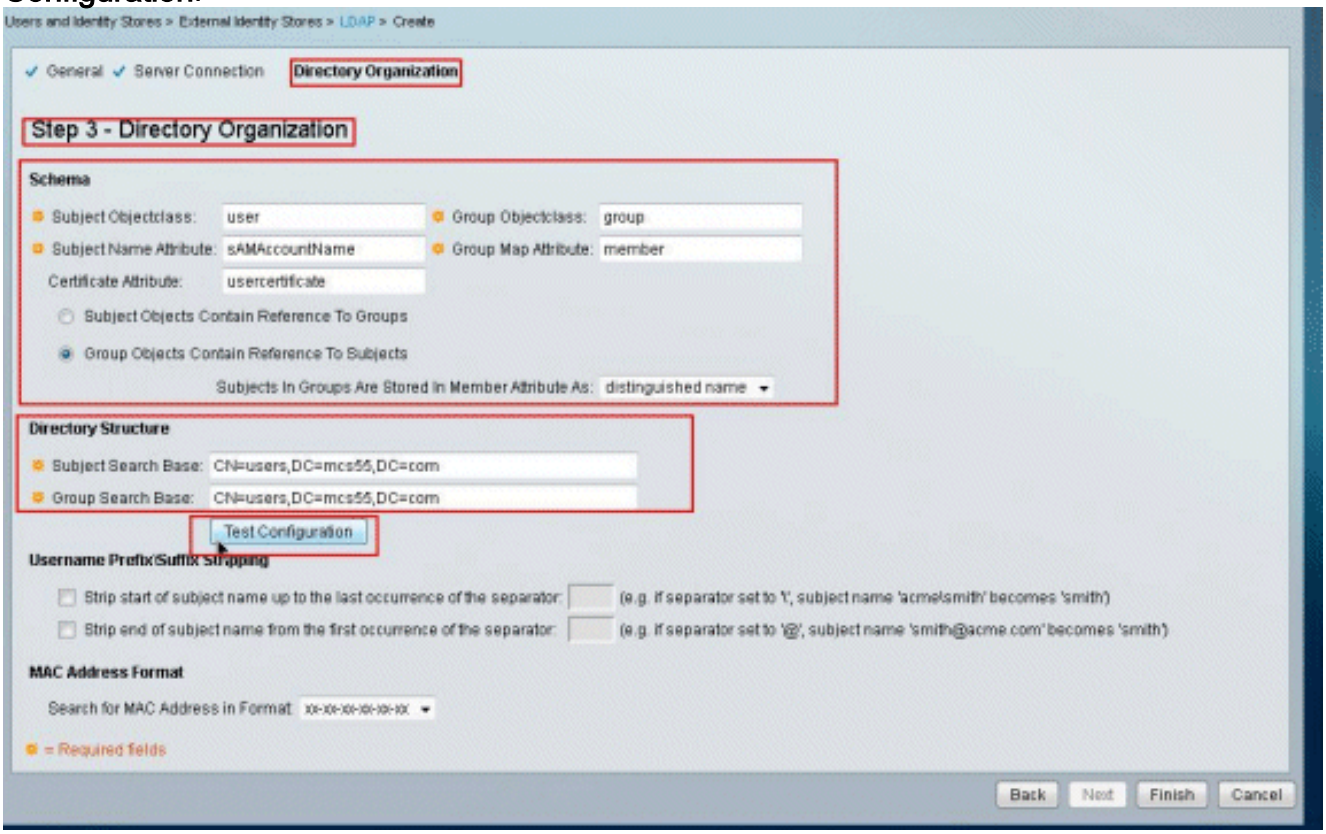


Opmerking: Als de Test Bind geen resultaat heeft, controleer dan de **Hostname**, **het poortnummer**, **Admin DN** en **Wachtwoord** van uw LDAP beheerder opnieuw.

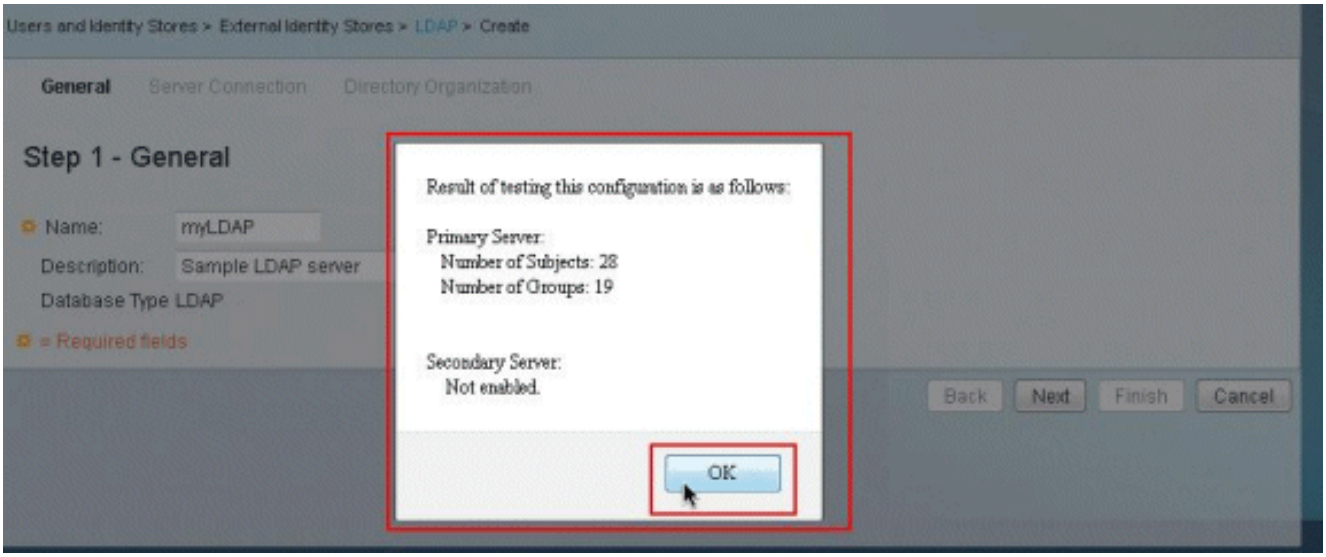
5. Klik op **Volgende**.



6. Geef de gewenste gegevens op in het tabblad Map onder de sectie Schema. Geef ook de vereiste informatie op onder het vak Map Structure zoals aangegeven door uw LDAP Admin. Klik op **Test Configuration**.

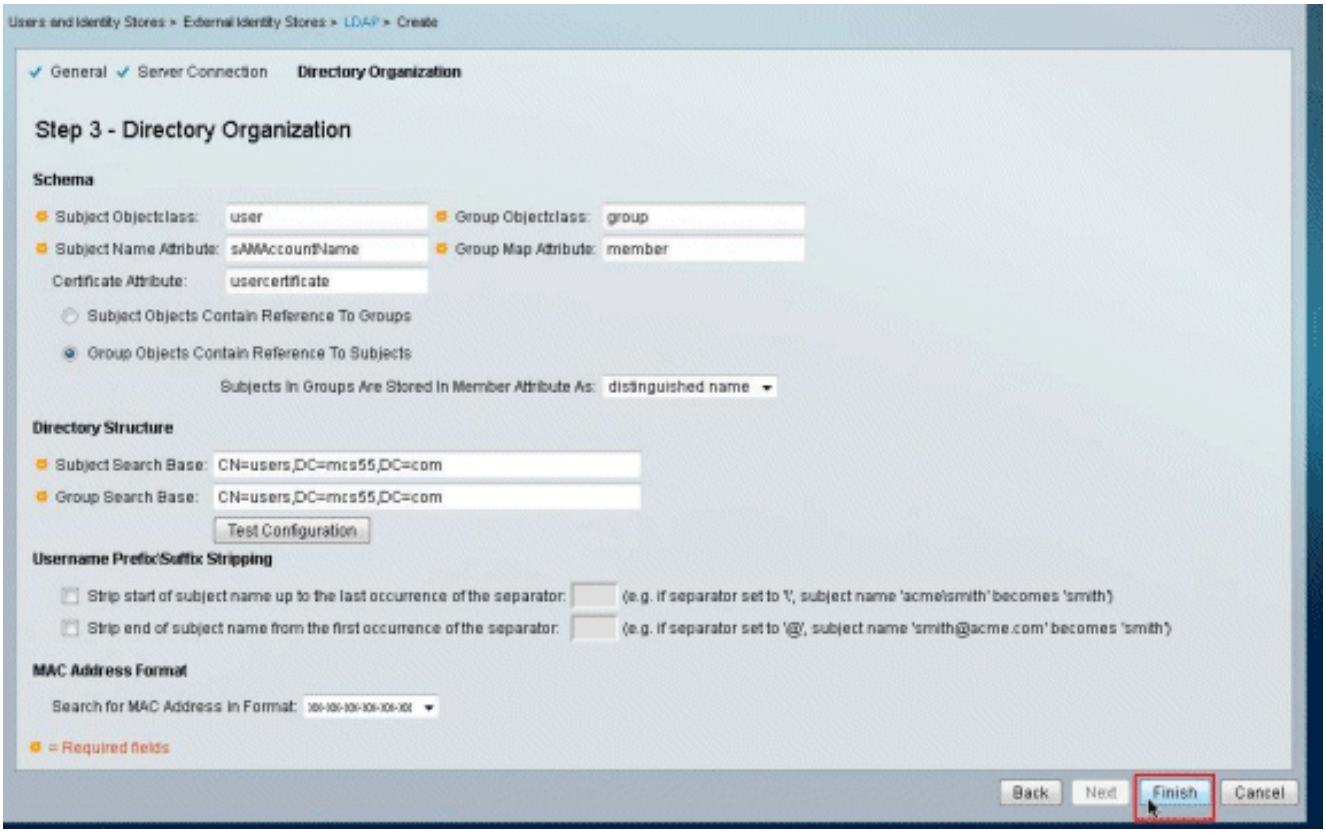


7. Deze afbeelding toont aan dat de **Configuration Test** is geslaagd.

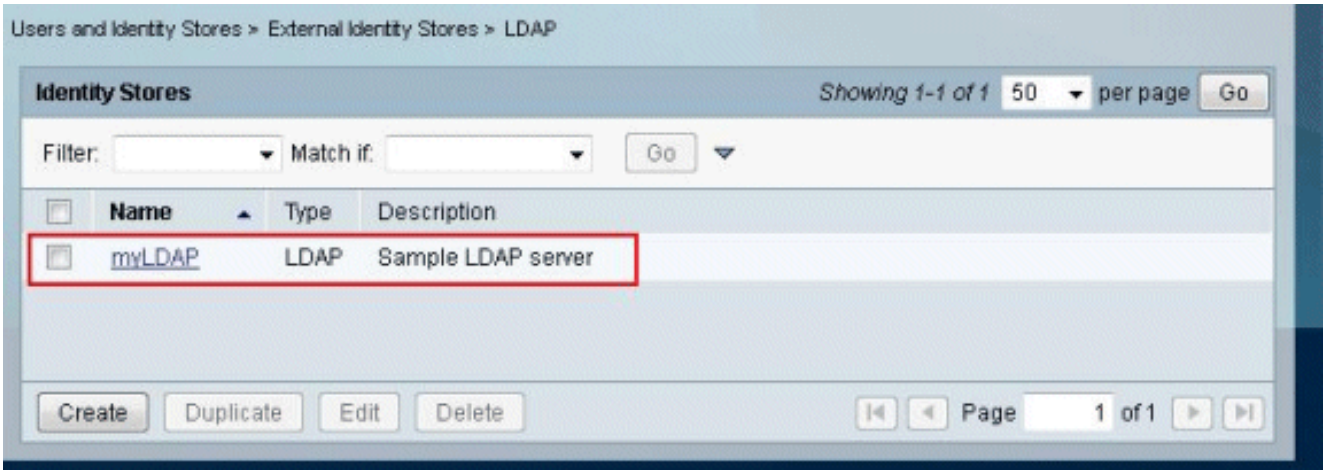


Opmerking: Als de Configuration Test geen resultaat heeft, controleert u de parameters in de **Schema** en de **Directory Structure** van uw LDAP-beheerder opnieuw.

8. Klik op **Voltooien**.

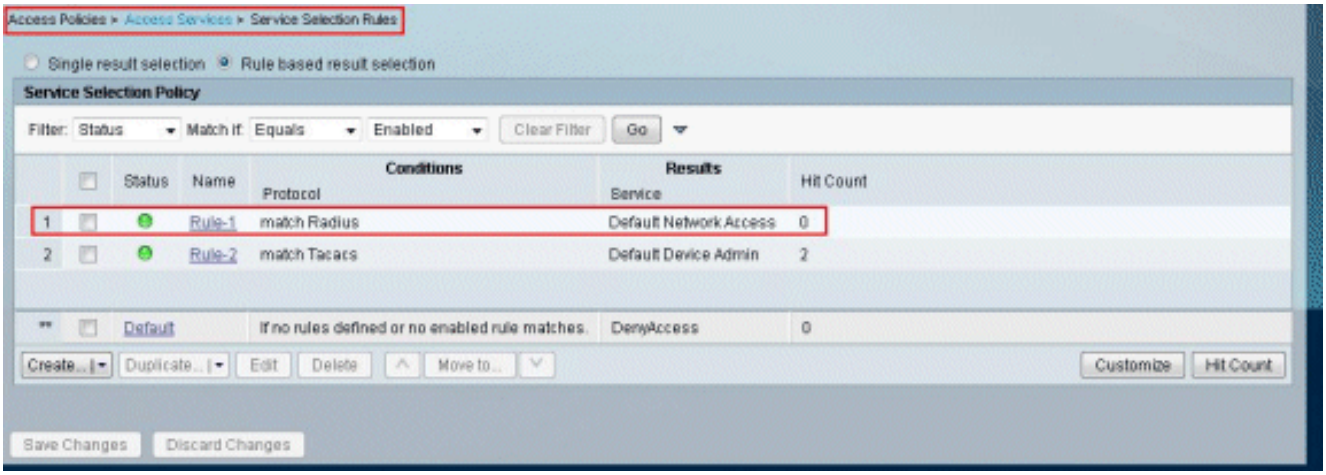


9. De **LDAP server** is gemaakt.

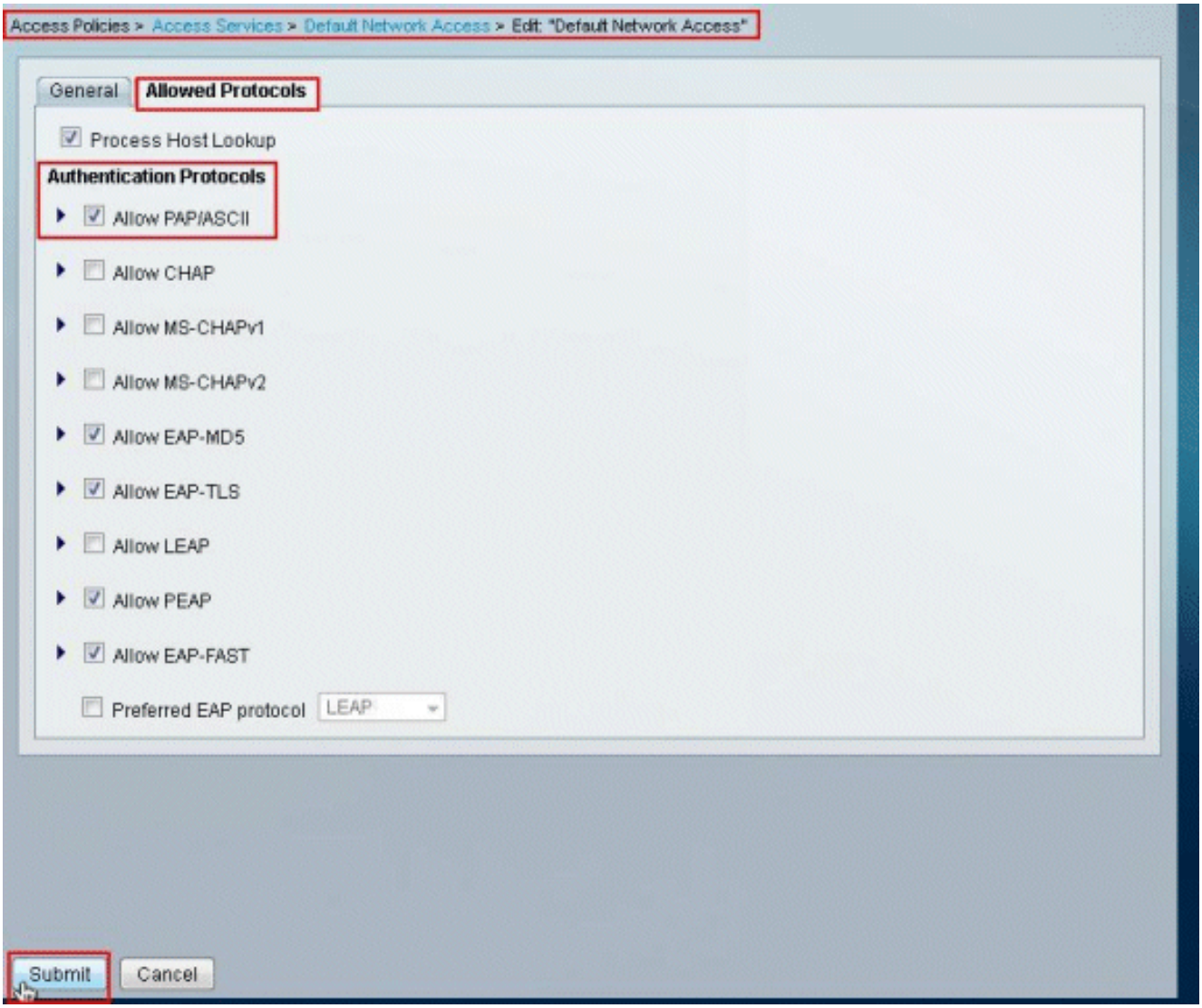


De Identity Store configureren

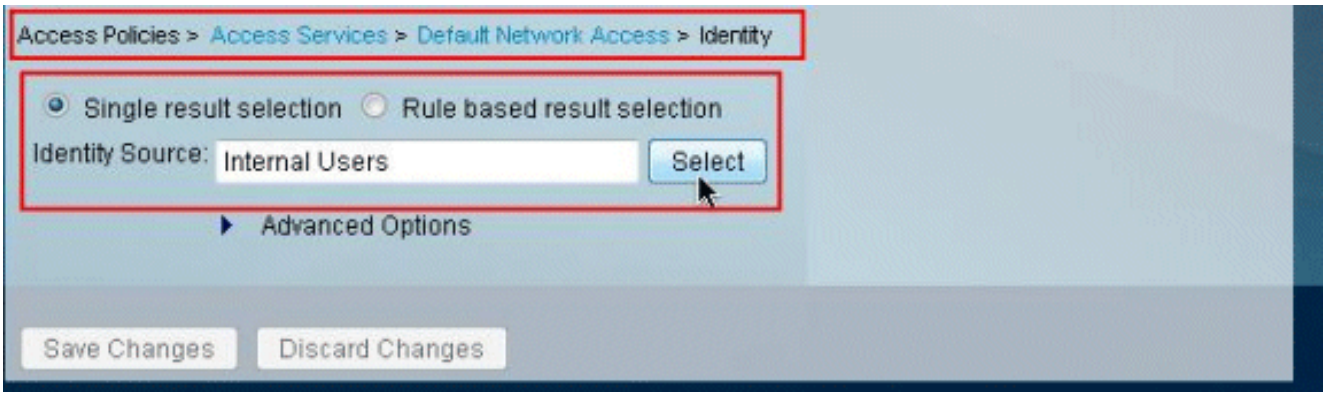
Om de Identity Store te configureren comprimeert u de stappen:

1. Kies **toegangsbeleid > Toegangsservices > regels voor servicesselectie** en controleer of de dienst de LDAP server voor verificatie gaat gebruiken. In dit voorbeeld gebruikt de LDAP Server verificatie de **Default Network Access**
   Service.
   

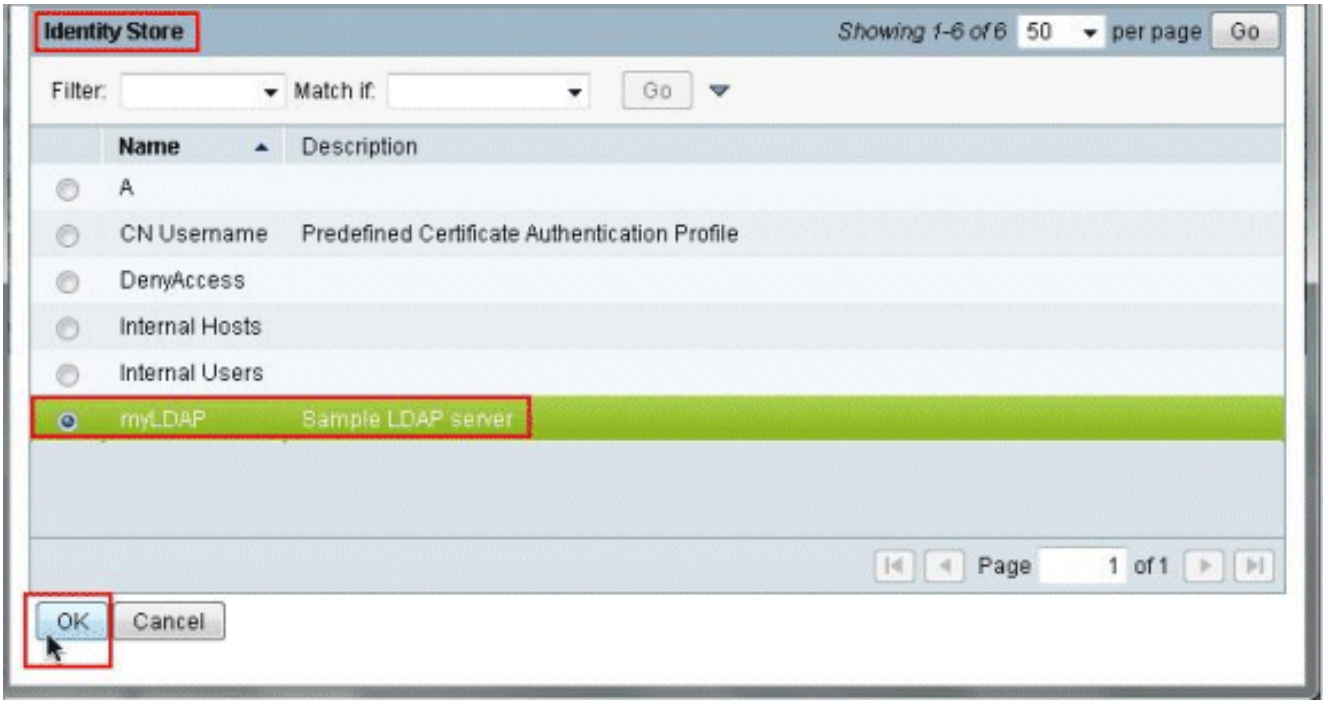
2. Nadat u de service in Stap 1 hebt geverifieerd, gaat u naar de specifieke service en klikt u op **Geautomatiseerde protocollen**. Zorg dat **PAP/ASCII** is geselecteerd en klik op **Indienen.Opmerking:** u kunt andere echtheidsprotocollen laten selecteren samen met Toegestaan
   PAP/ASCII.



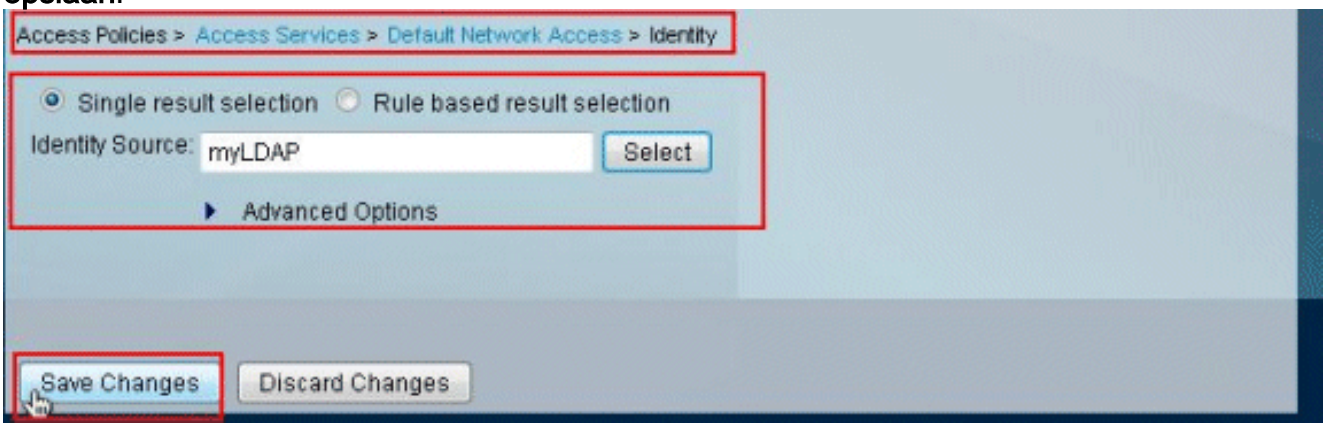
3. Klik op de service die in Stap 1 is geïdentificeerd en klik op **Identity**. Klik op **Selecteren** rechts van het veld Identity
Source.



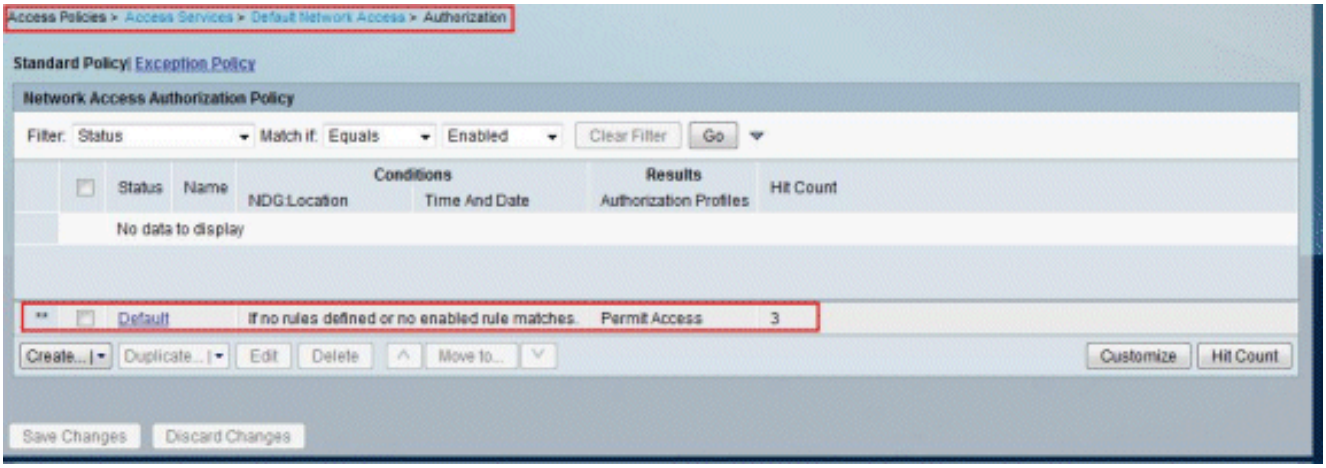
4. Selecteer de nieuwe LDAP-server (**mijn LDAP**, in dit voorbeeld) en klik op **OK**.



5. Klik op **Wijzigingen opslaan**.



6. Ga naar het gedeelte Automation van de service dat in Stap 1 is geïdentificeerd, en zorg ervoor dat er ten minste één regel is die **verificatie** toestaat.



Problemen oplossen

ACS stuurt een binair verzoek om de gebruiker te authentiseren tegen een LDAP server. Het bindt verzoek bevat het DNA van de gebruiker en het gebruikerswachtwoord in duidelijke tekst. Een

gebruiker is echt bevonden wanneer de DNA en het wachtwoord van de gebruiker overeenkomen met de gebruikersnaam en het wachtwoord in de LDAP-map.

- **Verificatiefouten** - ACS loggen verificatiefouten in de ACS-logbestanden.
- **Initialisatiefaciliteiten** - Gebruik de tijdinstellingen van de LDAP server om het aantal seconden te configureren dat ACS wacht op een antwoord van een LDAP server alvorens te bepalen dat de verbinding of verificatie op die server is mislukt. Mogelijke redenen voor de teruggave van een initialiseringsfout door een LDAP-server zijn:LDAP wordt niet ondersteundDe server is omlaagDe server is niet geheugenDe gebruiker heeft geen rechtenOnjuiste Administrator-referenties worden ingesteld
- **Bind fouten** - Mogelijke redenen voor een LDAP server om binden (authenticatie) fouten terug te geven zijn:FilterfoutenEen zoekopdracht met filtercriteria is misluktParameter foutenOngeldige parameters ingevoerdGebruikersaccount is beperkt (uitgeschakeld, uitgesloten, verlopen, verlopen, wachtwoord verlopen, enzovoort)

Deze fouten worden vastgelegd als externe resource fouten, wat wijst op een mogelijk probleem met de LDAP server:

- Er is een verbindingsfout opgetreden
- De termijn is verstreken
- De server is omlaag
- De server is niet geheugen

De `gebruiker A bestaat niet in de` fout `in de database` wordt geregistreerd als een onbekende gebruikersfout.

De fout `Een ongeldig wachtwoord is ingevoerd` als een ongeldig wachtwoord is inlogd als een fout met het wachtwoord, waar de gebruiker bestaat, maar het verzonden wachtwoord is ongeldig.

Gerelateerde informatie

- Cisco Secure Access Control-systeem
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems