ACS 5.x: Esempio di configurazione del server LDAP

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[Premesse](#)
[Servizio directory](#)
[Autenticazione tramite LDAP](#)
[Gestione connessione LDAP](#)
[Configurazione](#)
[Configurazione di ACS 5.x per LDAP](#)
[Configura l'archivio identità](#)
[Risoluzione dei problemi](#)
[Informazioni correlate](#)

Introduzione

Il protocollo LDAP (Lightweight Directory Access Protocol) è un protocollo di rete per l'esecuzione di query e la modifica dei servizi directory eseguiti su TCP/IP e UDP. LDAP è un meccanismo semplificato per l'accesso a un server delle directory basato su x.500. RFC 2251 definisce LDAP.

Cisco Secure Access Control System (ACS) 5.x si integra con un database esterno LDAP (detto anche archivio di identità) utilizzando il protocollo LDAP. Per la connessione al server LDAP sono disponibili due metodi: connessione in testo normale (semplice) e SSL (crittografata). È possibile configurare ACS 5.x per la connessione al server LDAP utilizzando entrambi questi metodi. In questo documento viene fornito un esempio di configurazione per la connessione di ACS 5.x a un server LDAP tramite una connessione semplice.

Prerequisiti

Requisiti

in questo documento si presume che ACS 5.x abbia una connessione IP al server LDAP e che la porta TCP 389 sia aperta.

Per impostazione predefinita, il server LDAP di Microsoft Active Directory è configurato per accettare le connessioni LDAP sulla porta TCP 389. Se si utilizza un altro server LDAP,

assicurarsi che sia attivo e in esecuzione e accettare le connessioni sulla porta TCP 389.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Servizio directory

Il servizio directory è un'applicazione software o un insieme di applicazioni utilizzate per memorizzare e organizzare le informazioni relative agli utenti e alle risorse di rete di un computer. È possibile utilizzare il servizio di elenco utenti per gestire l'accesso degli utenti a queste risorse.

Il servizio di directory LDAP si basa su un modello client-server. Un client si connette a un server LDAP per avviare una sessione LDAP e invia le richieste di operazione al server. Il server invia quindi le risposte. Uno o più server LDAP contengono i dati della struttura di directory LDAP o del database back-end LDAP.

Il servizio directory gestisce la directory, ovvero il database che contiene le informazioni. I servizi directory utilizzano un modello distribuito per archiviare le informazioni, che vengono in genere replicate tra i server delle directory.

Una directory LDAP è organizzata in una semplice gerarchia ad albero e può essere distribuita tra più server. Ogni server può disporre di una versione replicata della directory totale che viene sincronizzata periodicamente.

Una voce della struttura contiene un set di attributi, dove ogni attributo ha un nome (un tipo di attributo o una descrizione dell'attributo) e uno o più valori. Gli attributi sono definiti in uno schema.

Ogni voce dispone di un identificatore univoco denominato nome distinto (DN). Questo nome contiene il nome distinto relativo (RDN, Relative Distinguished Name) costruito dagli attributi nella voce, seguito dal DN della voce padre. Il DN può essere considerato come un nome di file completo e l'RDN come un nome di file relativo in una cartella.

Autenticazione tramite LDAP

ACS 5.x può autenticare un utente/gruppo/ruolo in base a un archivio di identità LDAP eseguendo un'operazione di binding sul server delle directory per trovare e autenticare l'utente/gruppo/ruolo. Se l'autenticazione ha esito positivo, ACS può recuperare i gruppi e gli attributi appartenenti all'utente/gruppo/ruolo. Gli attributi da recuperare possono essere configurati nell'interfaccia Web ACS (pagine LDAP). Questi gruppi e attributi possono essere utilizzati da ACS per autorizzare l'utente/gruppo/ruolo.

Per autenticare un utente o eseguire una query nell'archivio identità LDAP, ACS si connette al server LDAP e mantiene un connection pool. Vedere Gestione connessione LDAP.

Gestione connessione LDAP

ACS 5.x supporta più connessioni LDAP simultanee. Le connessioni vengono aperte su richiesta al momento della prima autenticazione LDAP. Il numero massimo di connessioni è configurato per ogni server LDAP. L'apertura anticipata delle connessioni riduce i tempi di autenticazione.

Èpossibile impostare il numero massimo di connessioni da utilizzare per le connessioni di binding simultanee. Il numero di connessioni aperte può essere diverso per ogni server LDAP (primario o secondario) e viene determinato in base al numero massimo di connessioni di amministrazione configurate per ogni server.

ACS conserva un elenco di connessioni LDAP aperte (incluse le informazioni sul binding) per ciascun server LDAP configurato in ACS. Durante il processo di autenticazione, la gestione connessione tenta di trovare una connessione aperta dal pool.

Se non esiste una connessione aperta, ne viene aperta una nuova. Se il server LDAP ha chiuso la connessione, la gestione connessione segnala un errore durante la prima chiamata per la ricerca nella directory e tenta di rinnovare la connessione.

Al termine del processo di autenticazione, la gestione connessione rilascia la connessione alla gestione connessione. Per ulteriori informazioni, consultare la Guida dell'utente di ACS 5.X.

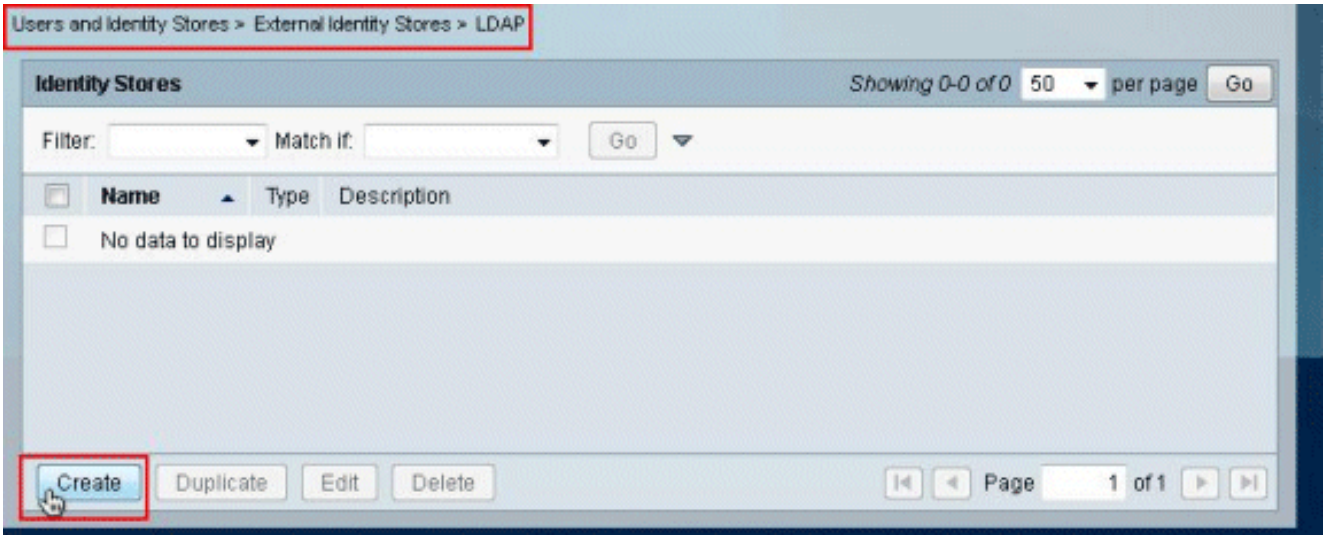
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

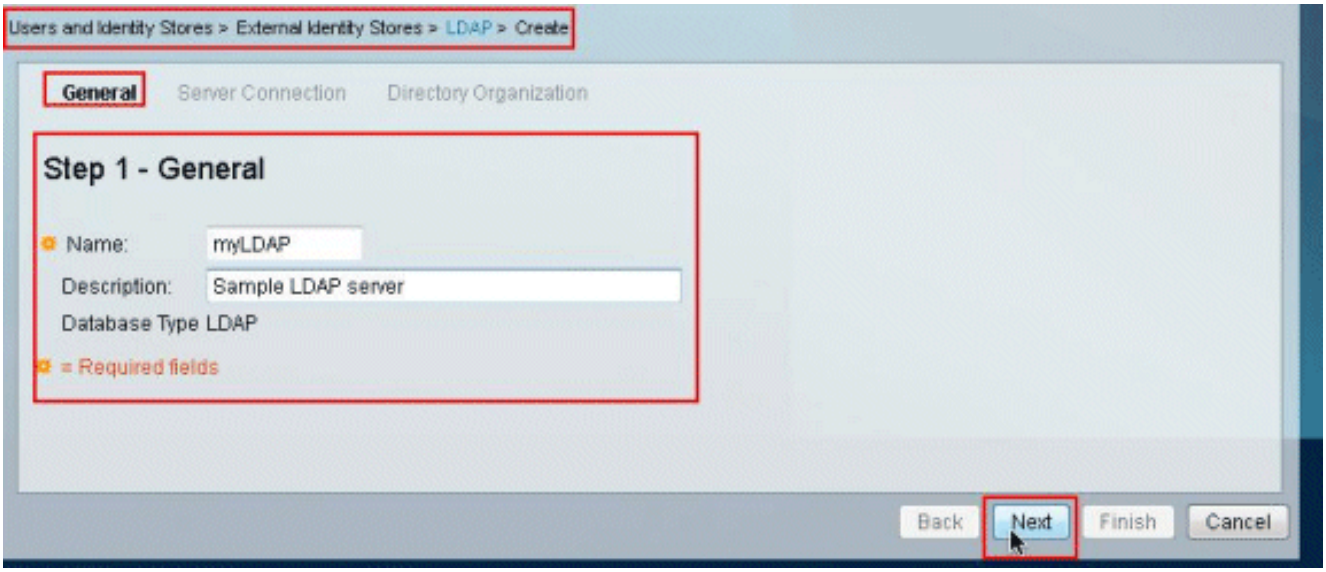
Configurazione di ACS 5.x per LDAP

Completare questa procedura per configurare ACS 5.x per LDAP:

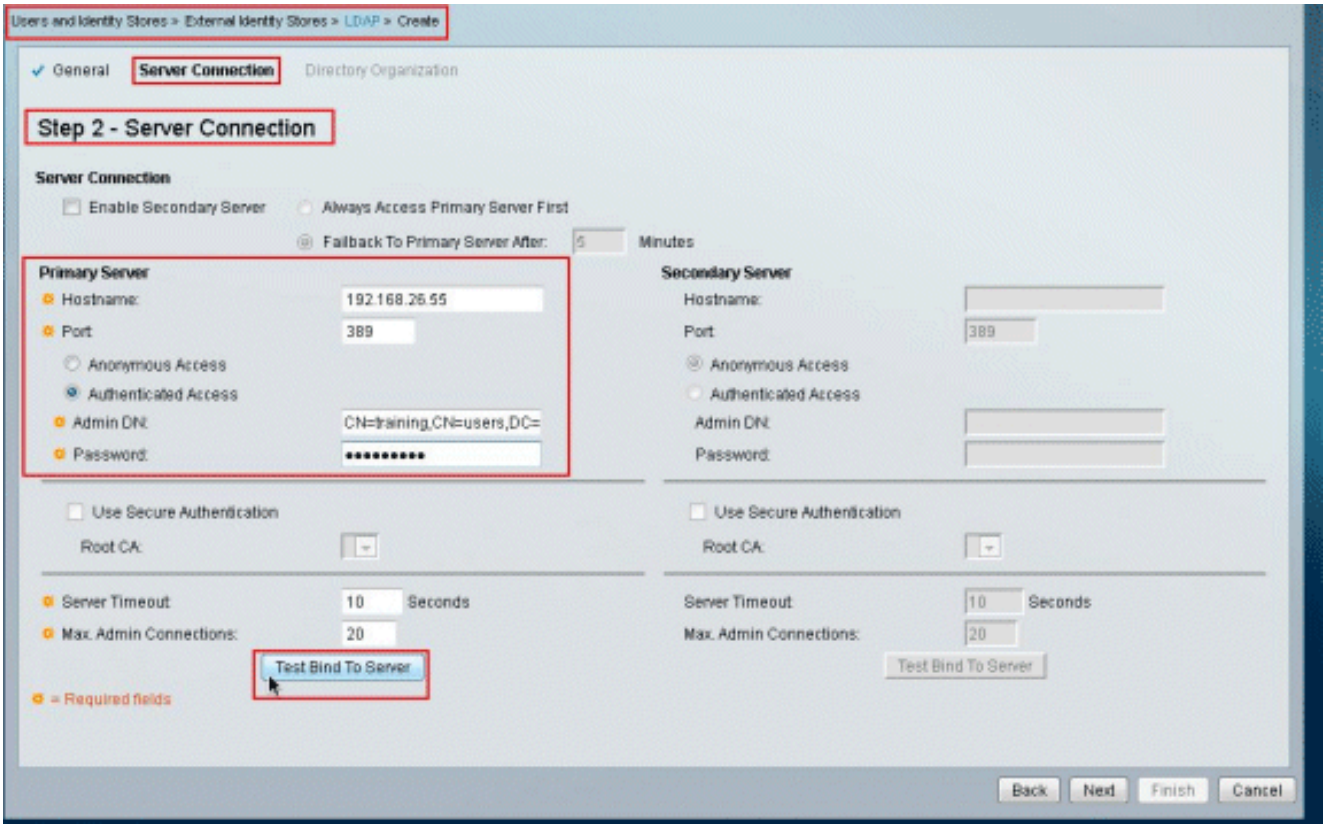
1. Scegliere **Utenti e archivi identità > Archivi identità esterni > LDAP**, quindi fare clic su **Crea** per creare una nuova connessione
   LDAP.



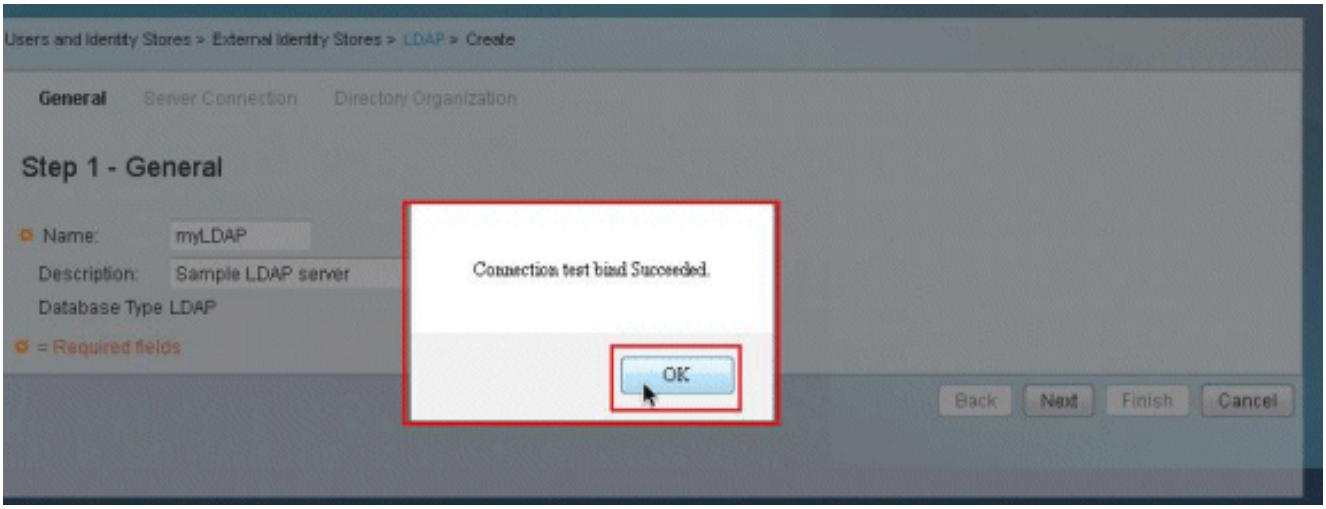
2. Nella scheda Generale, fornire il **Nome** e la **Descrizione** (facoltativi) per il nuovo LDAP e fare clic su
Avanti.



3. Nella scheda Connessione server della sezione Server primario specificare **Nome host**, **Porta**, **DN amministratore** e **Password**. Fare clic su **Test binding a server**.**Nota:** il numero di porta assegnato da IANA per LDAP è TCP 389. Tuttavia, confermare il numero di porta utilizzato dal server LDAP dall'amministratore LDAP. Il DN e la password dell'amministratore devono essere forniti dall'amministratore LDAP. Il DN amministratore deve disporre di tutte le autorizzazioni di lettura per tutte le unità organizzative nel server
LDAP.

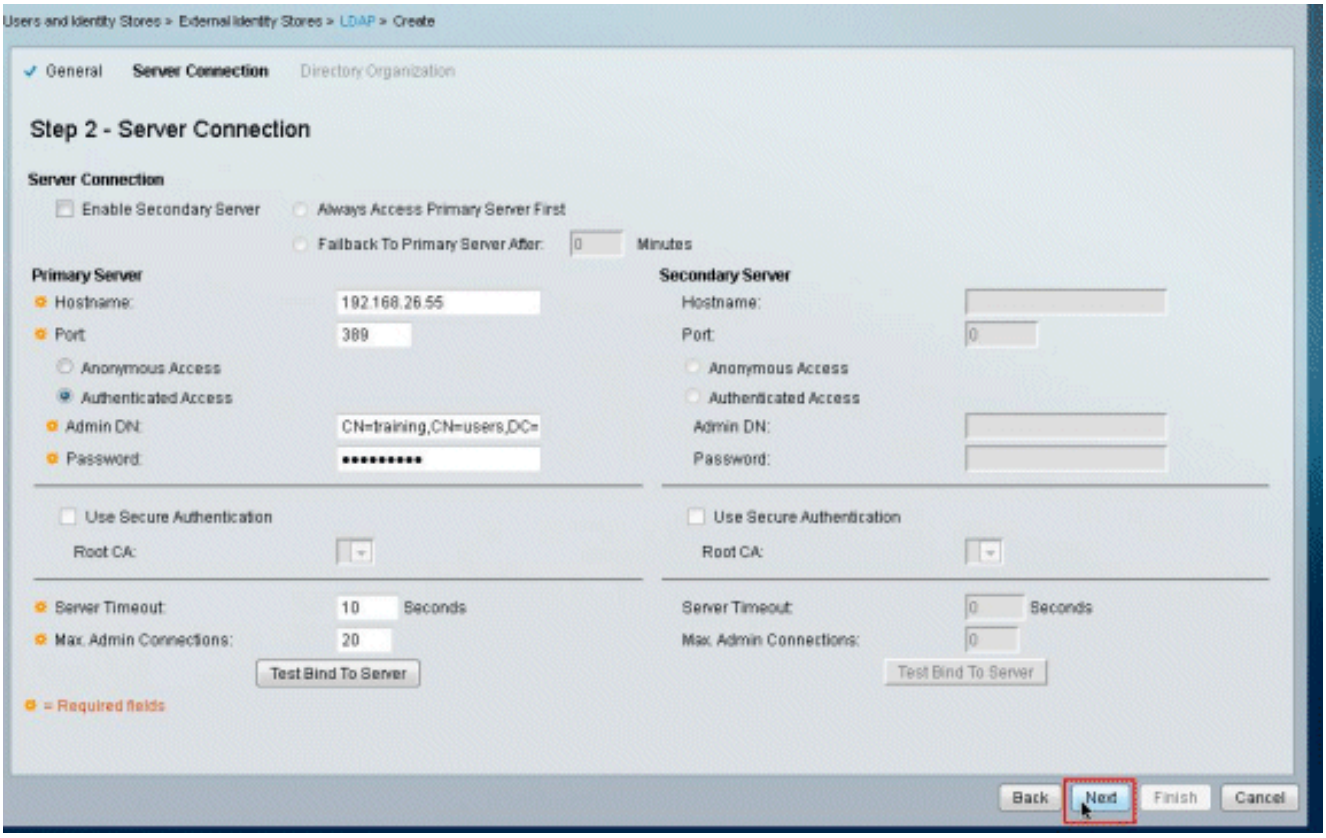


4. In questa immagine viene mostrato che l'**associazione del test di connessione al server** è riuscita.

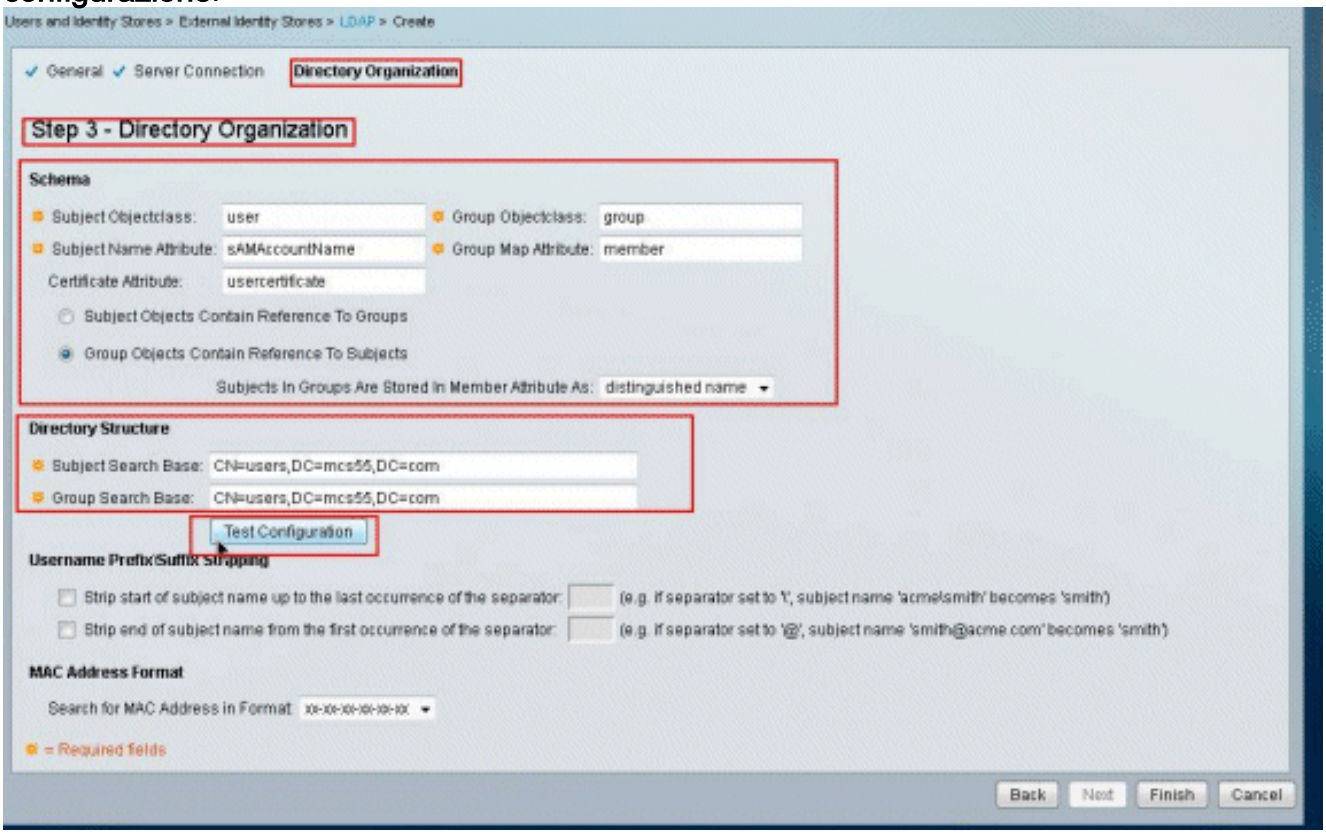


Nota: se il test di binding ha esito negativo, verificare nuovamente **Nome host**, **Numero porta**, **DN amministratore** e **Password** dall'amministratore LDAP.

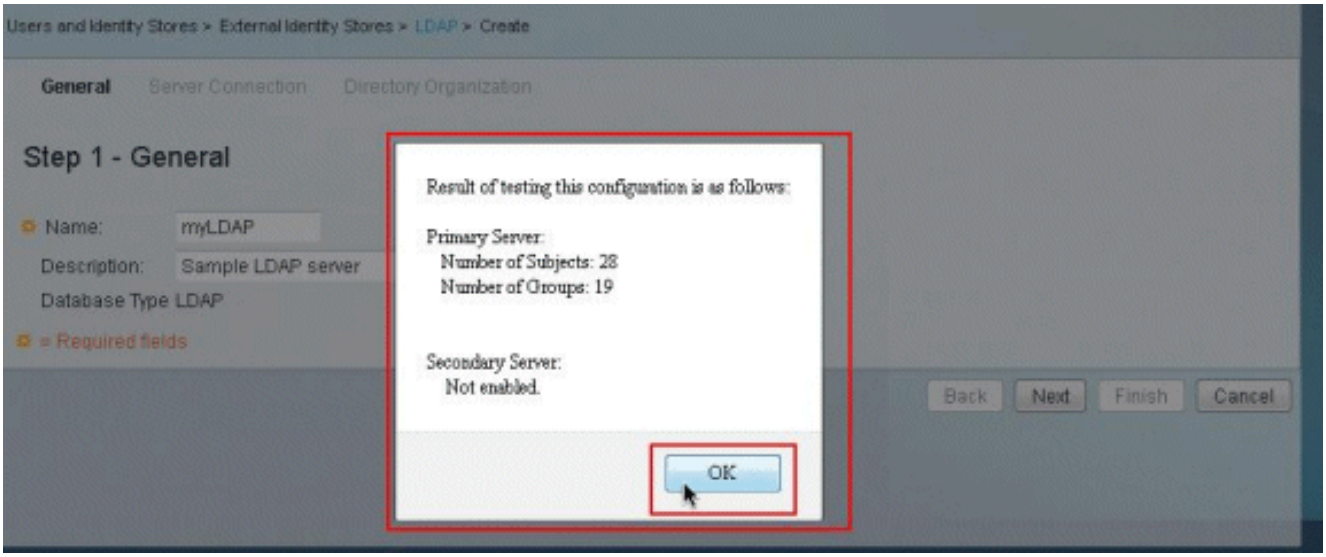
5. Fare clic su **Next**
(Avanti).



6. Specificare i dettagli richiesti nella scheda Organizzazione directory della sezione Schema. Analogamente, fornire le informazioni richieste nella sezione Struttura directory come fornito dall'amministratore LDAP. Fare clic su **Test configurazione**.

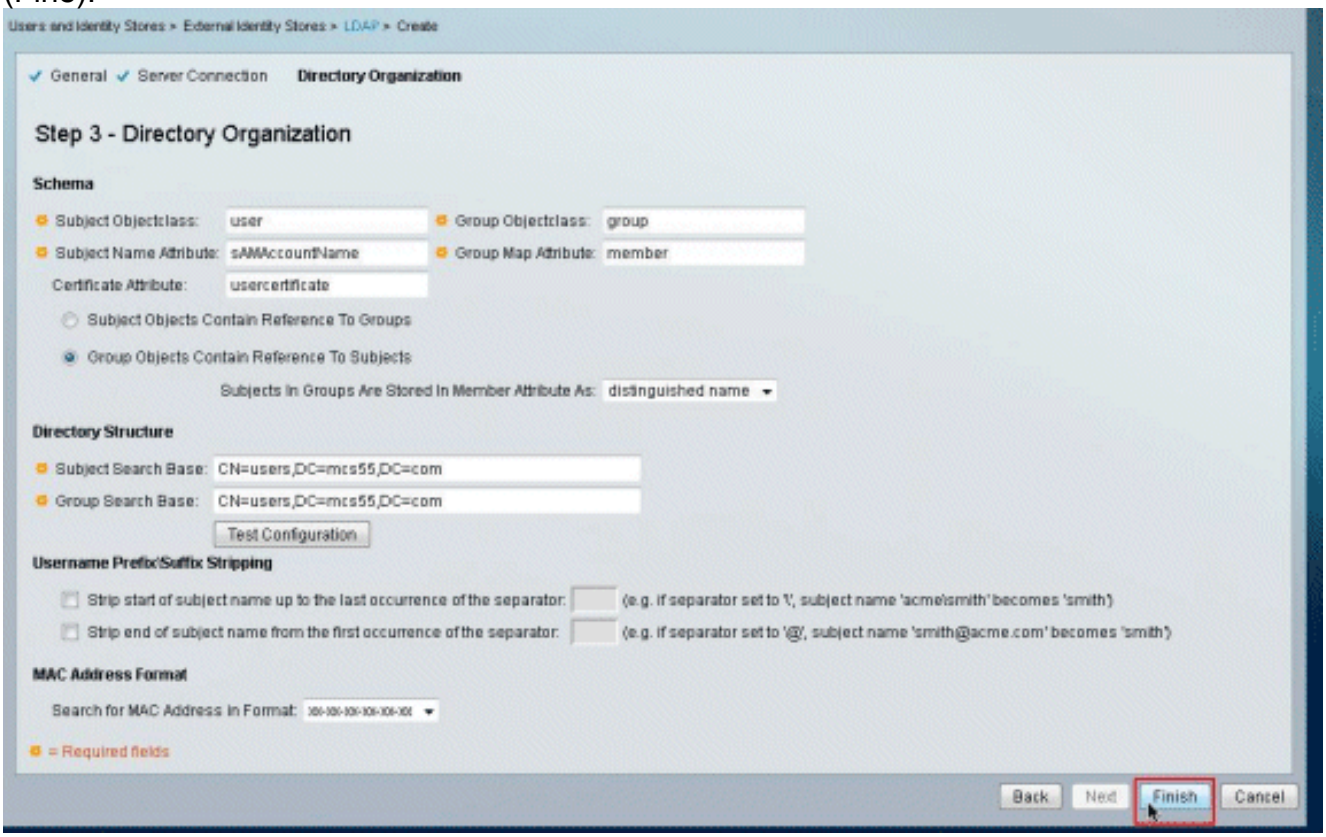


7. Nell'immagine viene mostrato che il **test di configurazione** è riuscito.

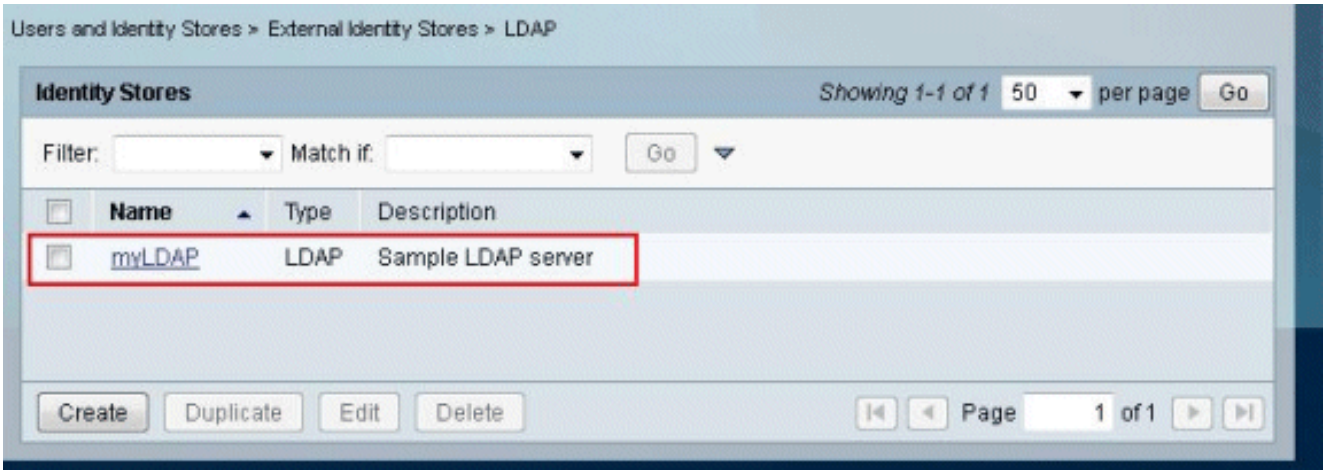


Nota: se il test Configuration non viene superato, verificare nuovamente i parametri forniti nello **schema** e nella **struttura di directory** dall'amministratore LDAP.

8. Fare clic su **Finish**
   (Fine).



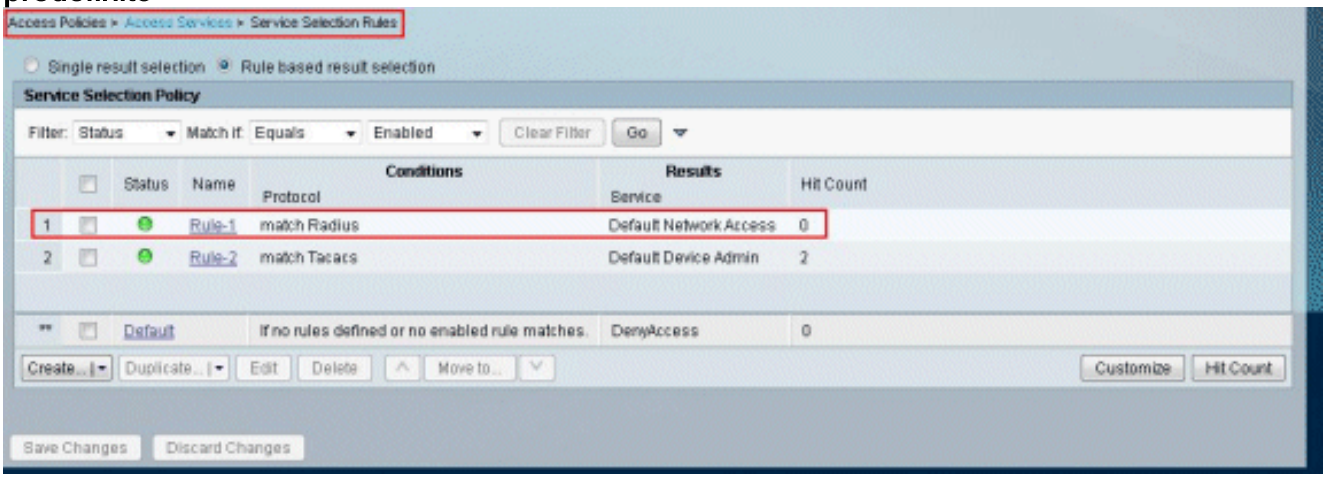
9. Creazione del **server LDAP**
   completata.



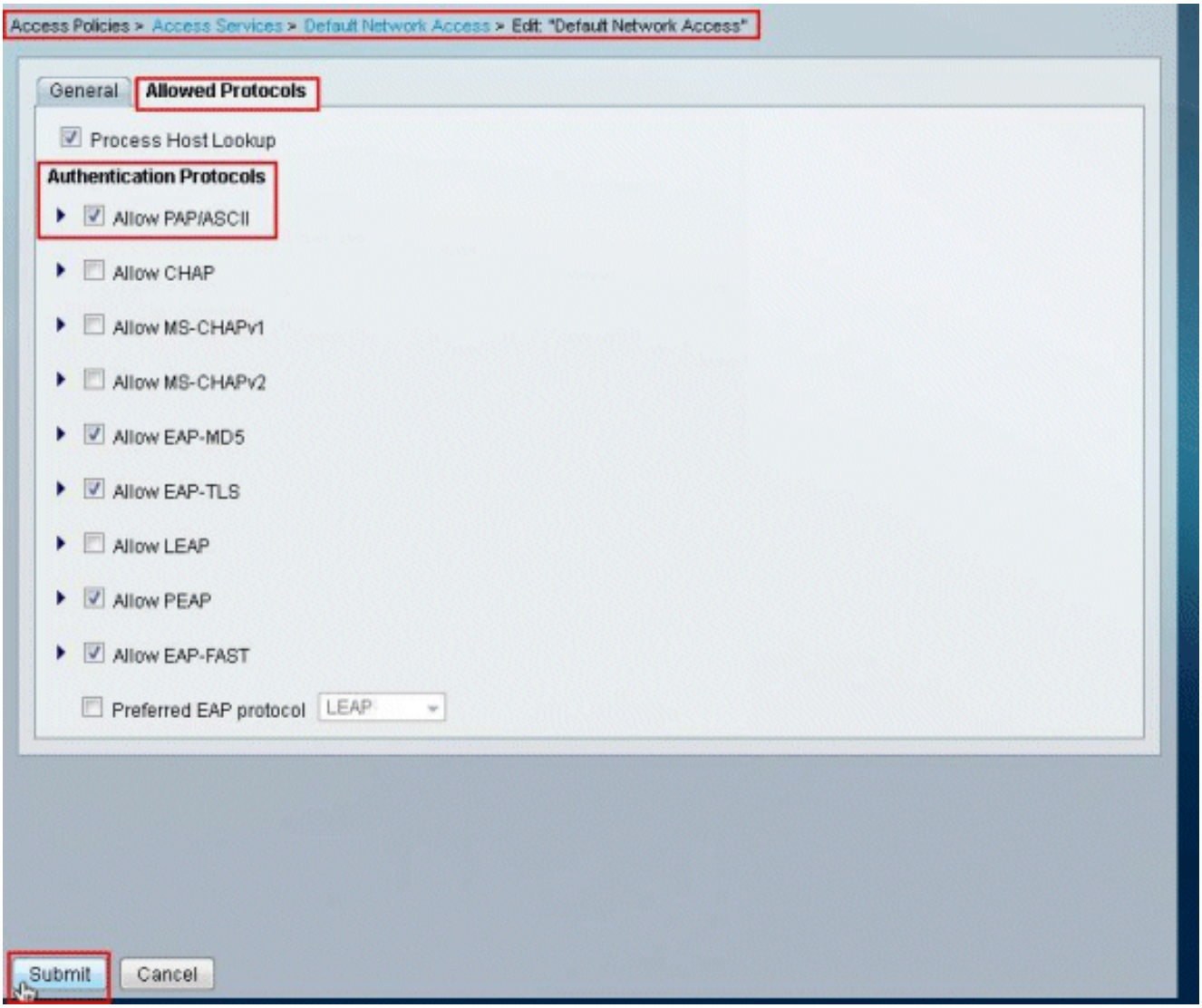
Configura l'archivio identità

Completare i passaggi per configurare l'archivio identità:

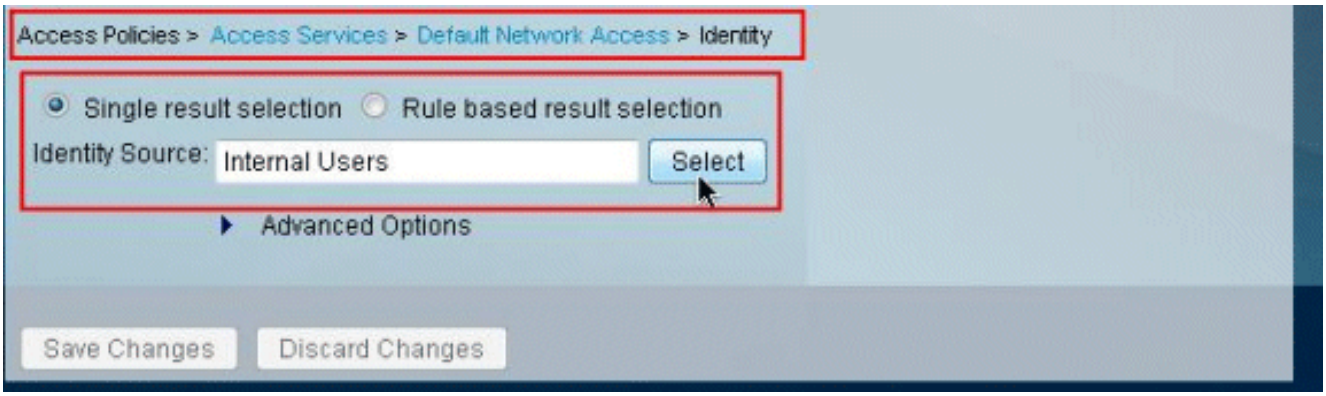
1. Scegliere **Criteri di accesso > Servizi di accesso > Regole selezione servizio** e verificare quale servizio utilizzerà il server LDAP per l'autenticazione. In questo esempio, l'autenticazione del server LDAP utilizza il servizio **Accesso alla rete predefinito**.



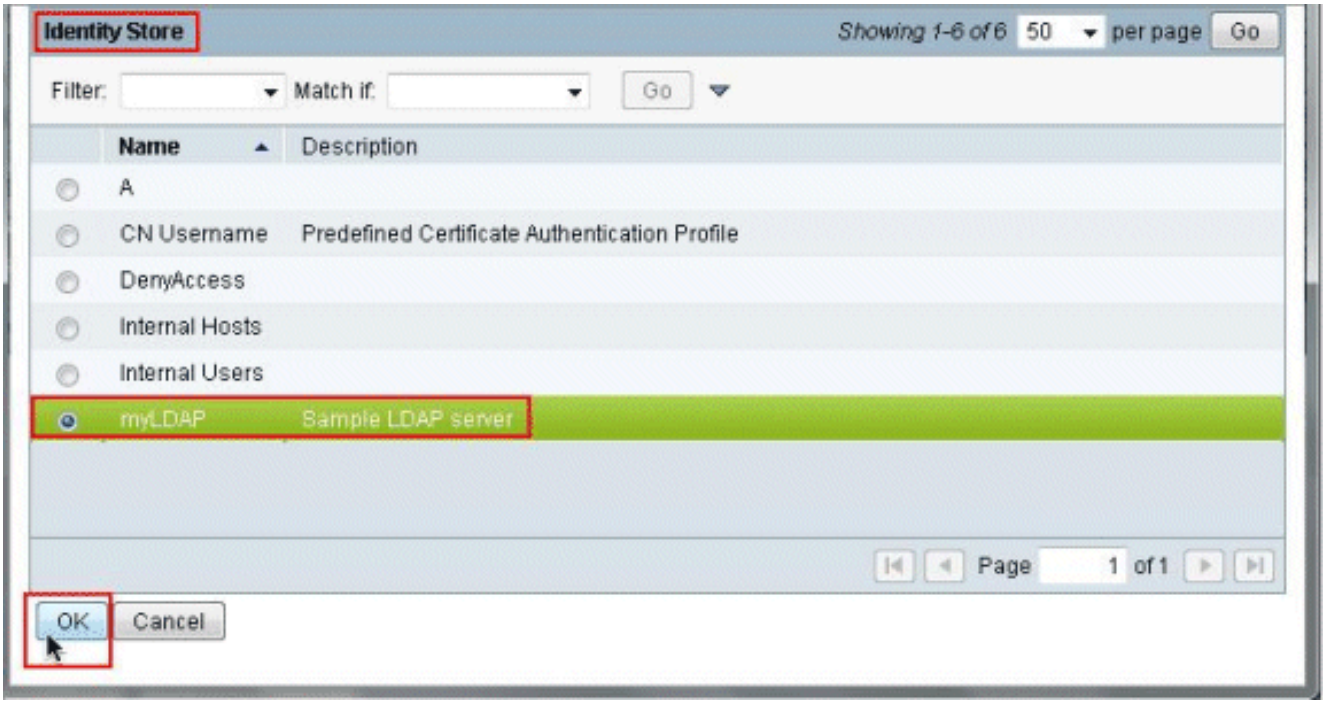
2. Una volta verificato il servizio al punto 1, passare al servizio specifico e fare clic su **Protocolli consentiti**. Verificare che l'opzione **Allow PAP/ASCII** sia selezionata, quindi fare clic su **Submit** (Invia).**Nota: è** possibile selezionare altri protocolli di autenticazione insieme a Allow PAP/ASCII.



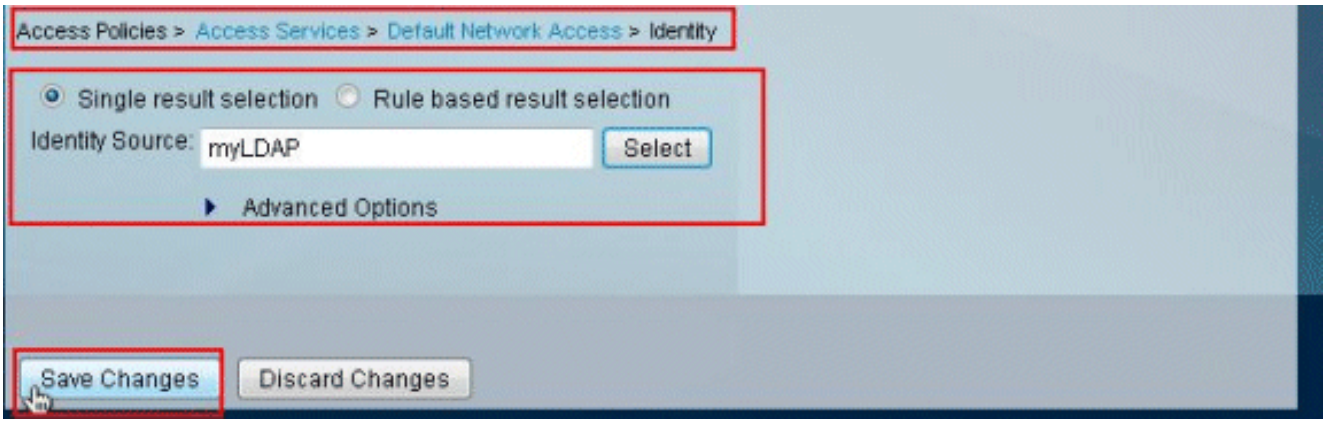
3. Fare clic sul servizio identificato nel passo 1, quindi fare clic su **Identità**. Fare clic su **Seleziona** a destra del campo Origine identità.



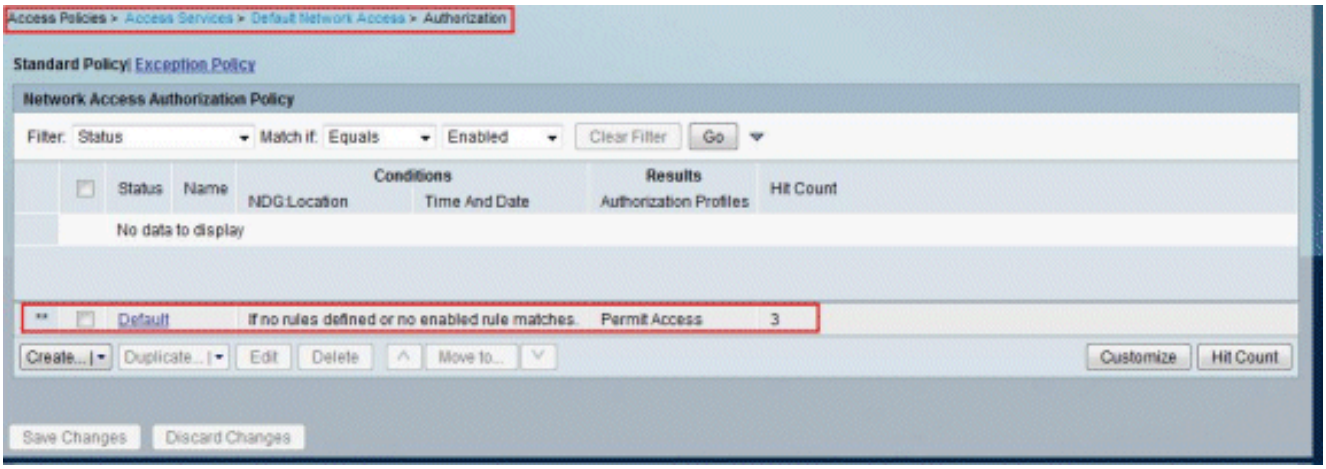
4. Selezionare il server LDAP appena creato (**myLDAP**, in questo esempio) e fare clic su **OK**.



5. Fare clic su **Salva modifiche**.



6. Andare alla sezione Autorizzazione del servizio identificato nel passaggio 1 e verificare che sia presente almeno una regola che consente l'**autenticazione**.



Risoluzione dei problemi

ACS invia una richiesta di binding per autenticare l'utente su un server LDAP. La richiesta di binding contiene il DN e la password dell'utente in testo non crittografato. Un utente viene

autenticato quando il DN e la password dell'utente corrispondono al nome utente e alla password nella directory LDAP.

- **Errori di autenticazione**: ACS registra gli errori di autenticazione nei file di registro ACS.
- **Errori di inizializzazione**: utilizzare le impostazioni di timeout del server LDAP per configurare il numero di secondi di attesa da parte di ACS di una risposta da un server LDAP prima di stabilire se la connessione o l'autenticazione su tale server non è riuscita. I possibili motivi per cui un server LDAP restituisce un errore di inizializzazione sono:LDAP non supportatoIl server non è attivoMemoria del server insufficienteL'utente non dispone di privilegiSono state configurate credenziali di amministratore non corrette
- **Errori di binding** - Possibili motivi per cui un server LDAP restituisce errori di binding (autenticazione):Errori di filtroUna ricerca che utilizza criteri di filtro non riesceErrori parametriSono stati immessi parametri non validiL'account utente è soggetto a restrizioni (disabilitato, bloccato, scaduto, password scaduta e così via)

Questi errori vengono registrati come errori di risorse esterne, indicando un possibile problema con il server LDAP:

- Errore di connessione
- Timeout scaduto
- Il server non è attivo
- Memoria del server insufficiente

L'`utente A non esiste nell'`errore `del database` viene registrato come errore di tipo Utente sconosciuto.

L'errore `Password non valida immessa` viene registrato come Password non valida, dove l'utente esiste, ma la password inviata non è valida.

Informazioni correlate

- Cisco Secure Access Control System
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems