ACS 5.X: Esempio di configurazione del server LDAP sicuro

Sommario

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 il protocollo LDAP.

Access Control Server (ACS) 5.x si integra con un database esterno LDAP, detto anche archivio di identità, utilizzando il protocollo LDAP. Esistono due metodi per connettersi al server LDAP: connessione in testo normale (semplice) e SSL (crittografata). È possibile configurare ACS 5.x per la connessione al server LDAP utilizzando entrambi i metodi. In questo documento ACS 5.x è configurato per la connessione a un server LDAP tramite connessione crittografata.

Prerequisiti

Requisiti

in questo documento si presume che ACS 5.x abbia una connessione IP al server LDAP e che la porta TCP 636 sia aperta.

Il server LDAP Microsoft® Active Directory deve essere configurato in modo da accettare connessioni LDAP sicure sulla porta TCP 636. In questo documento si presume che l'utente disponga del certificato radice dell'Autorità di certificazione (CA) che ha rilasciato il certificato del server al server LDAP Microsoft. Per ulteriori informazioni su come configurare il server LDAP, consultare il documento sulla modalità di abilitazione di LDAP su SSL con un'autorità di

certificazione di terze parti.

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 che consente di memorizzare e organizzare le informazioni relative agli utenti e alle risorse di rete di un computer. È possibile utilizzare il servizio directory per gestire l'accesso degli utenti a queste risorse.

Il servizio di directory LDAP si basa su un modello client-server. Un client avvia una sessione LDAP connettendosi a un server 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 l'archiviazione delle 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 ha un identificatore univoco: il relativo 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.

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 per l'utente di ACS 5.X.

Configurazione

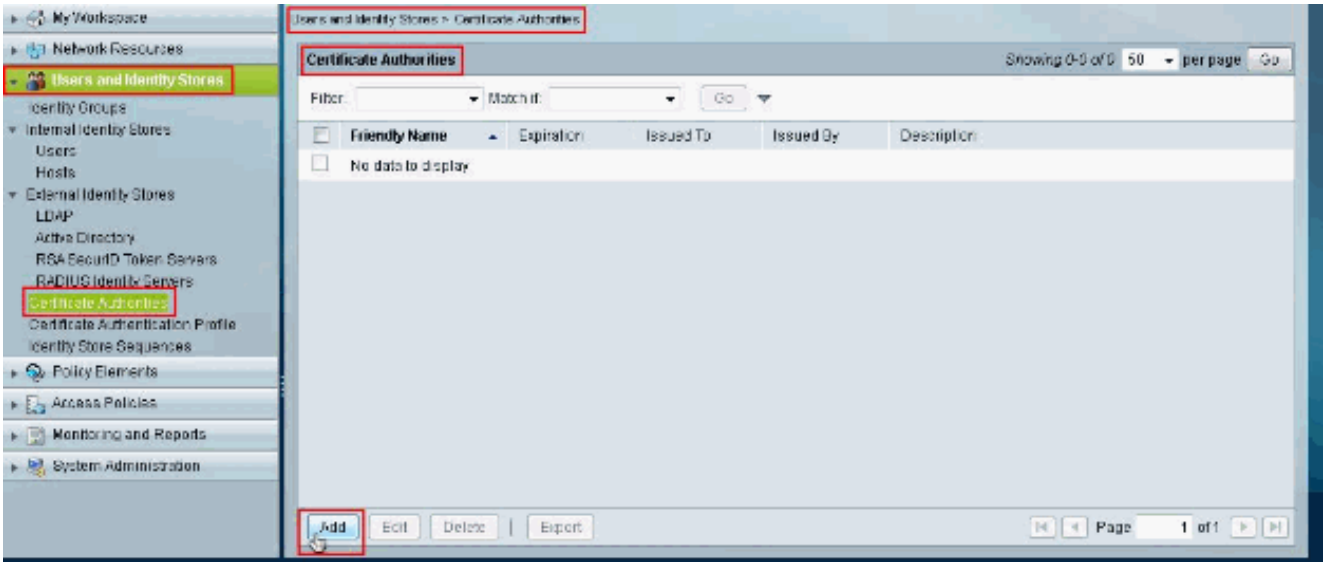
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Installa certificato CA radice in ACS 5.x

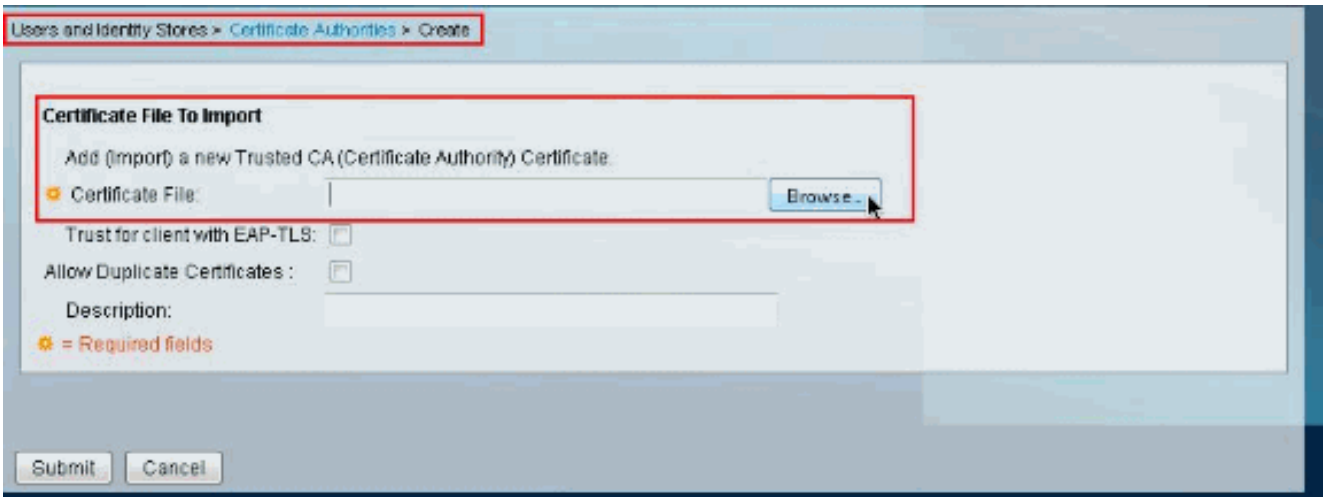
Completare questa procedura per installare un certificato CA radice su Cisco Secure ACS 5.x:

Nota: verificare che il server LDAP sia preconfigurato per accettare connessioni crittografate sulla porta TCP 636. Per ulteriori informazioni su come configurare il server LDAP Microsoft, vedere Come abilitare LDAP su SSL con un'autorità di certificazione di terze parti.

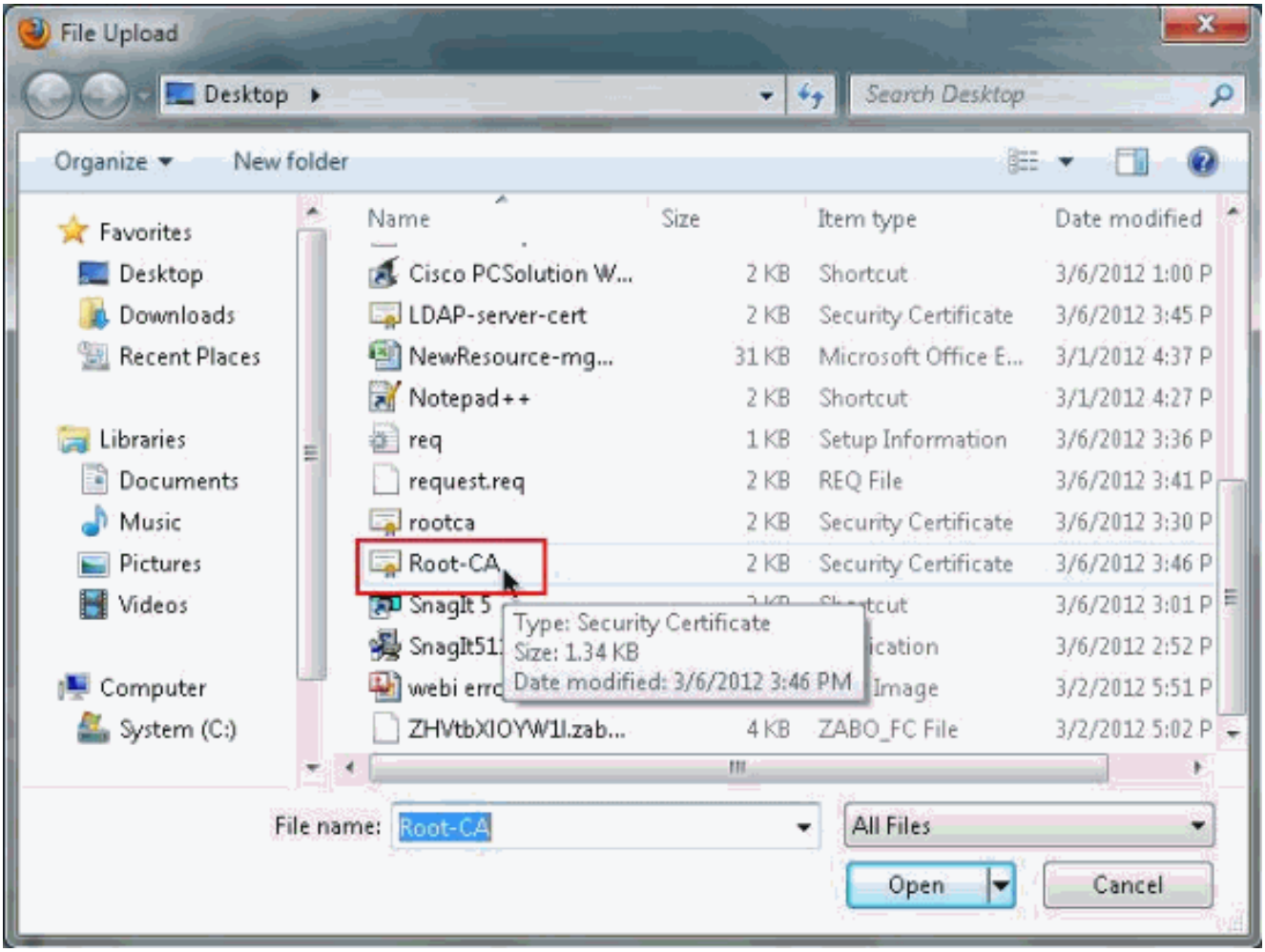
1. Scegliere **Utenti e archivi identità > Autorità di certificazione**, quindi fare clic su **Aggiungi** per aggiungere il certificato radice della CA che ha emesso il certificato del server al server LDAP
   Microsoft.



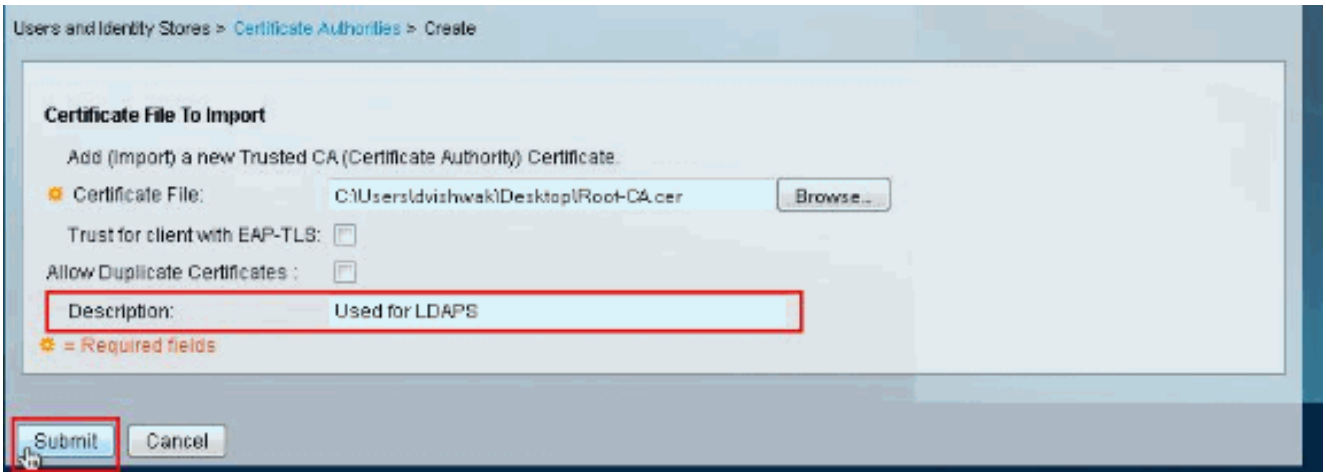
2. Dalla sezione **File certificato da importare** fare clic su **Sfoglia** accanto a **File certificato** per cercare il file
certificato.



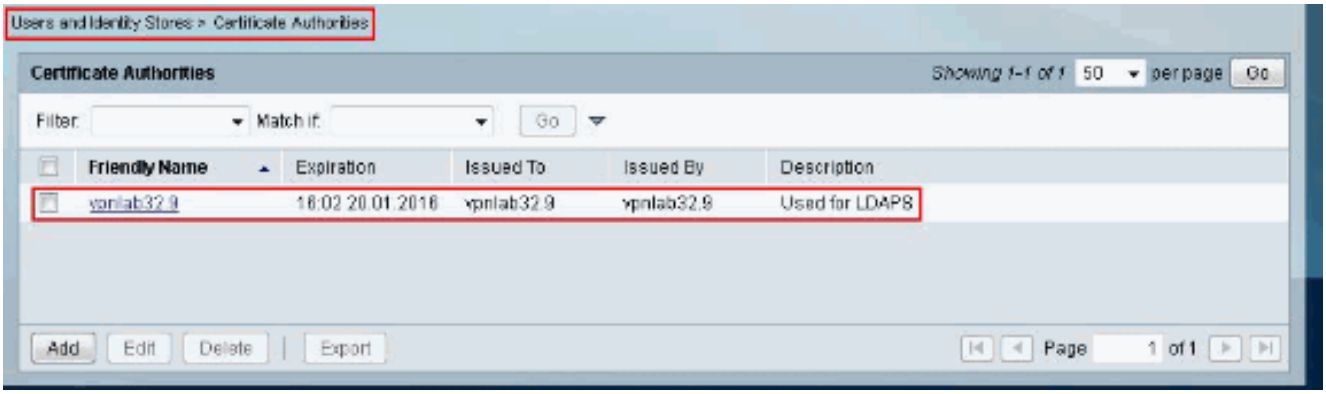
3. Scegliere il **file del certificato** richiesto (il certificato radice della CA che ha rilasciato il certificato del server al server LDAP Microsoft) e fare clic su
Apri.



4. Specificare una **descrizione** nello spazio disponibile accanto a Descrizione e fare clic su **Invia**.



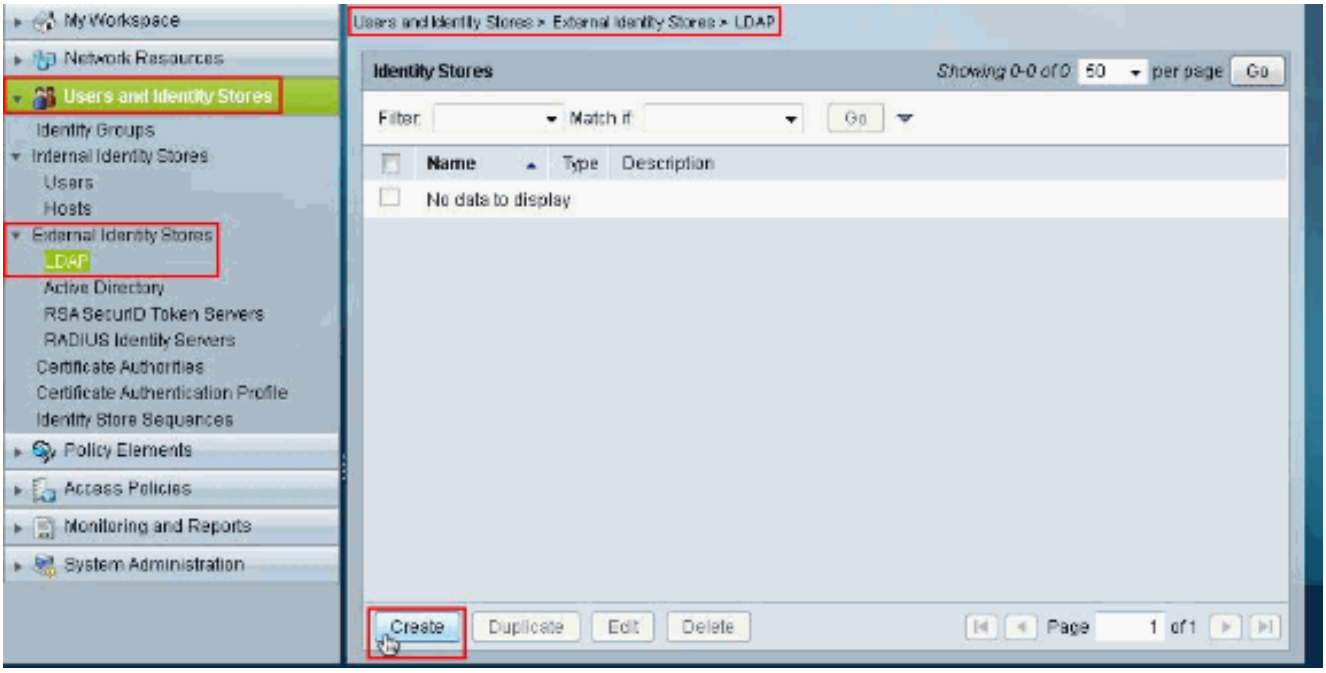
Nell'immagine viene mostrato che il certificato radice è stato installato correttamente:



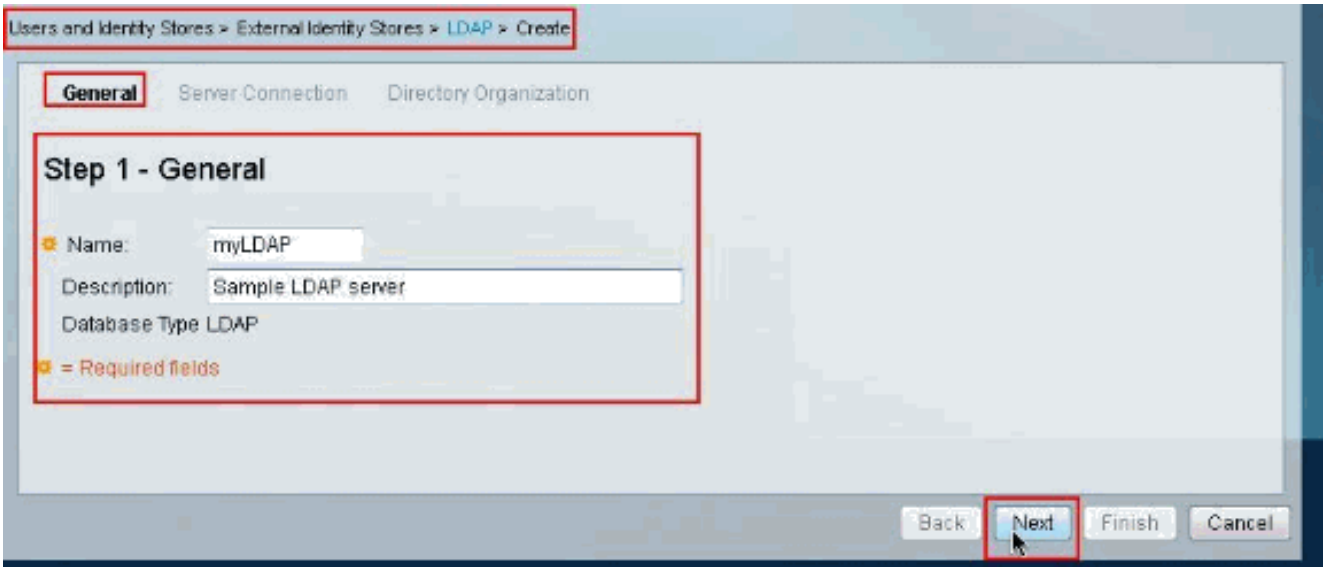
Configurazione di ACS 5.X per LDAP protetto

Completare questa procedura per configurare ACS 5.x per il protocollo LDAP sicuro:

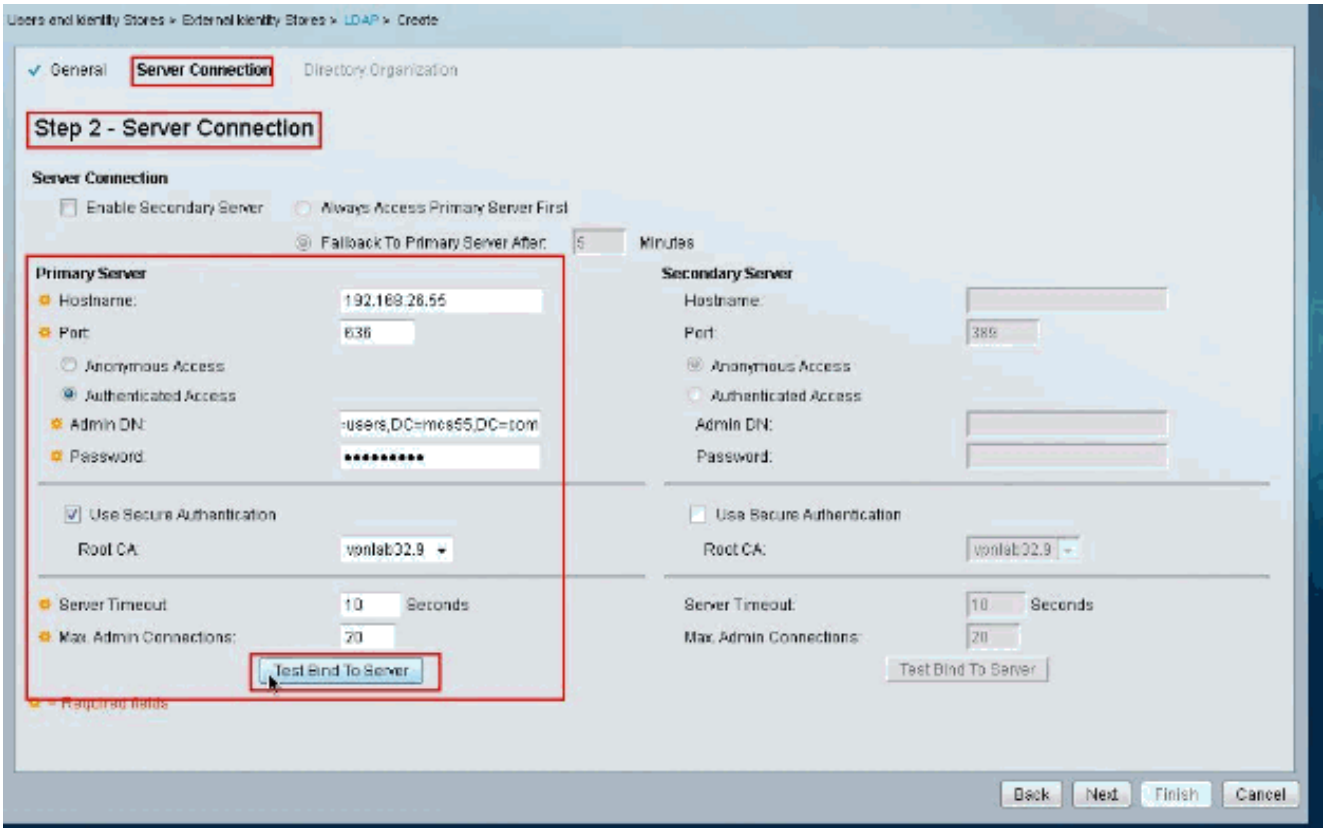
1. Scegliere **Utenti e archivi identità > Archivi identità esterni > LDAP** e fare clic su **Crea** per creare una nuova connessione
   LDAP.



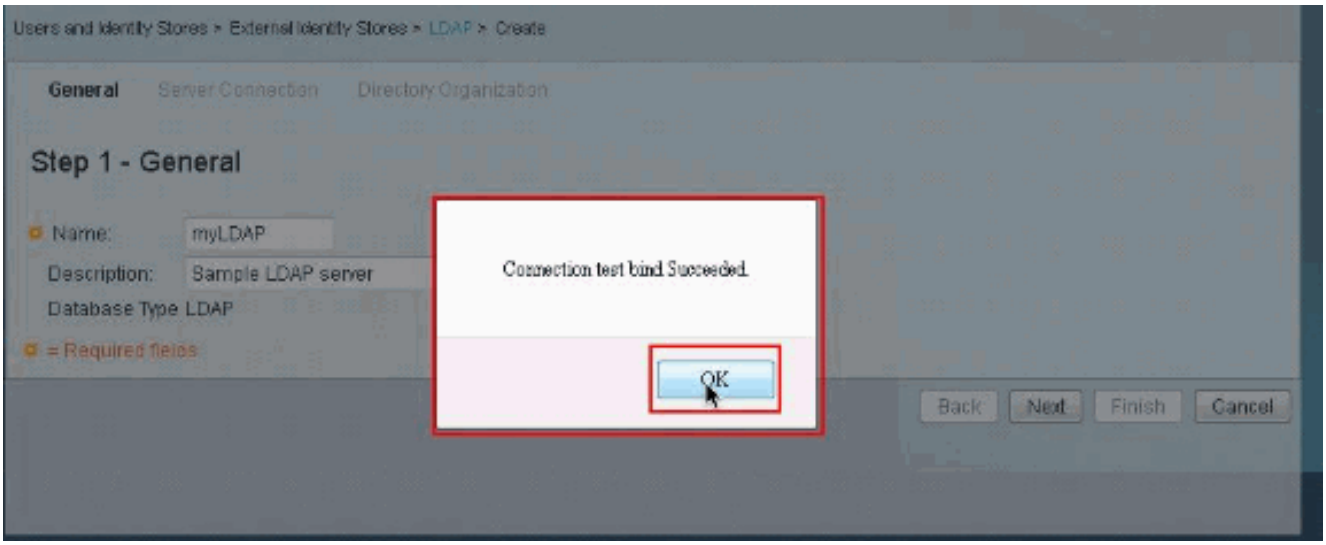
2. Dalla scheda **Generale** fornire il **Nome** e la **Descrizione** (facoltativa) per il nuovo LDAP, quindi fare clic su
   Avanti.



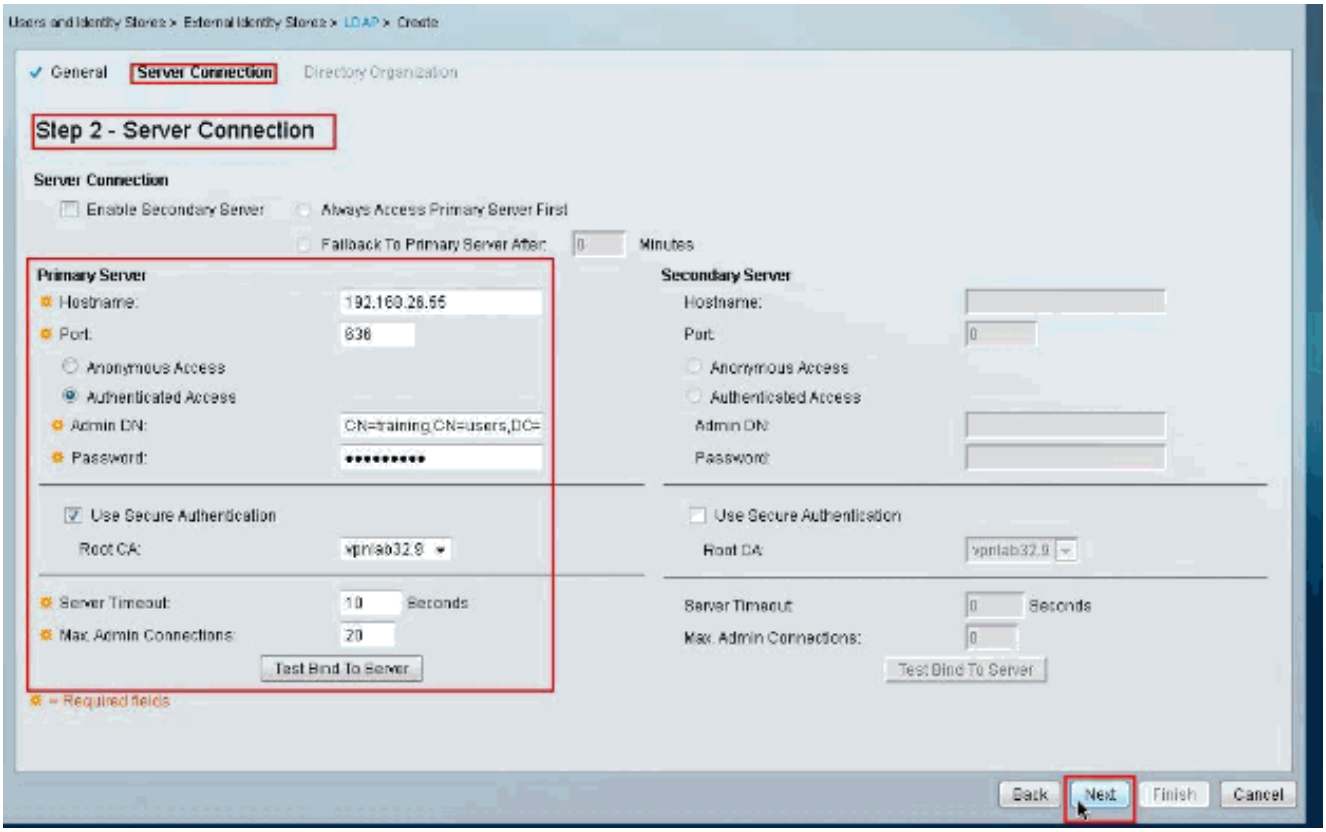
3. Dalla scheda **Connessione server** della sezione **Server primario**, specificare il **nome host, la porta, il DN e la password di amministrazione**. Verificare che la casella di controllo accanto a **Usa autenticazione protetta** sia selezionata e scegliere il **certificato CA radice** installato di recente. Fare clic su **Test binding a server**.**Nota:** il numero di porta assegnato da IANA per LDAP protetto è TCP 636. Tuttavia, confermare il numero di porta utilizzato dal server LDAP dall'amministratore LDAP.**Nota:** il DN e la password dell'amministratore devono essere forniti dall'amministratore LDAP. Il DN amministratore deve disporre di autorizzazioni di lettura per tutte le unità organizzative nel server
   LDAP.



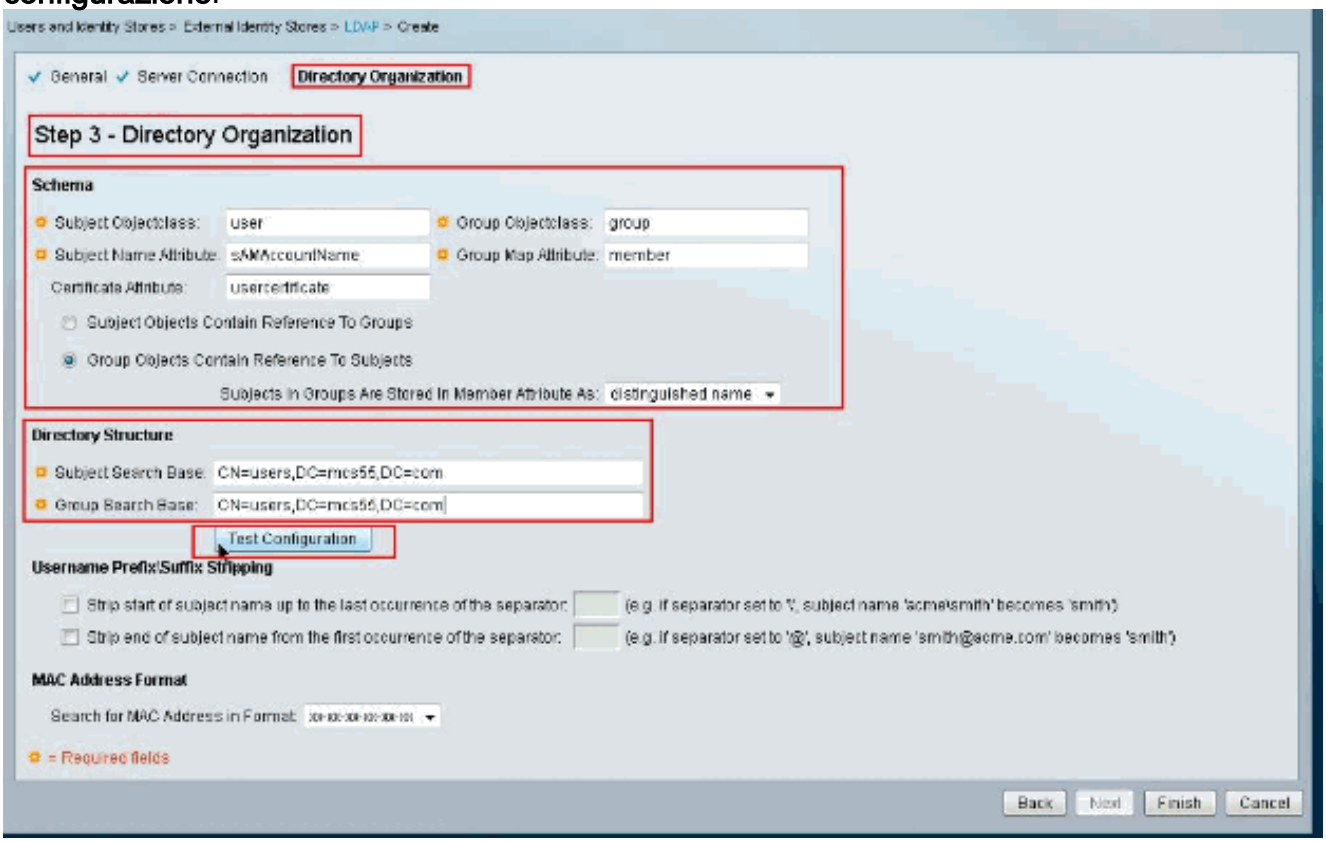
Nell'immagine seguente viene mostrato che l'**associazione del test di connessione al server** è riuscita.**Nota:** se il test di binding ha esito negativo, verificare nuovamente il **nome host, il numero di porta, il DN di amministrazione, la password** e la **CA radice** dall'amministratore LDAP.



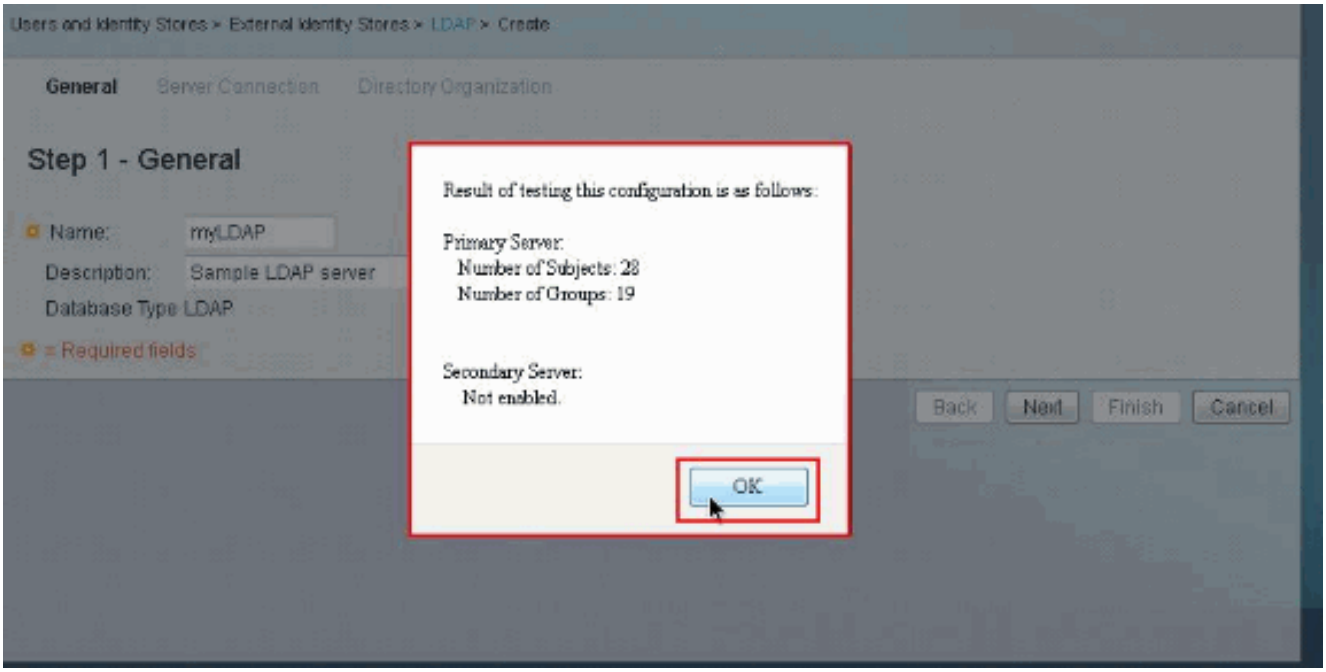
4. Fare clic su **Next**
   (Avanti).



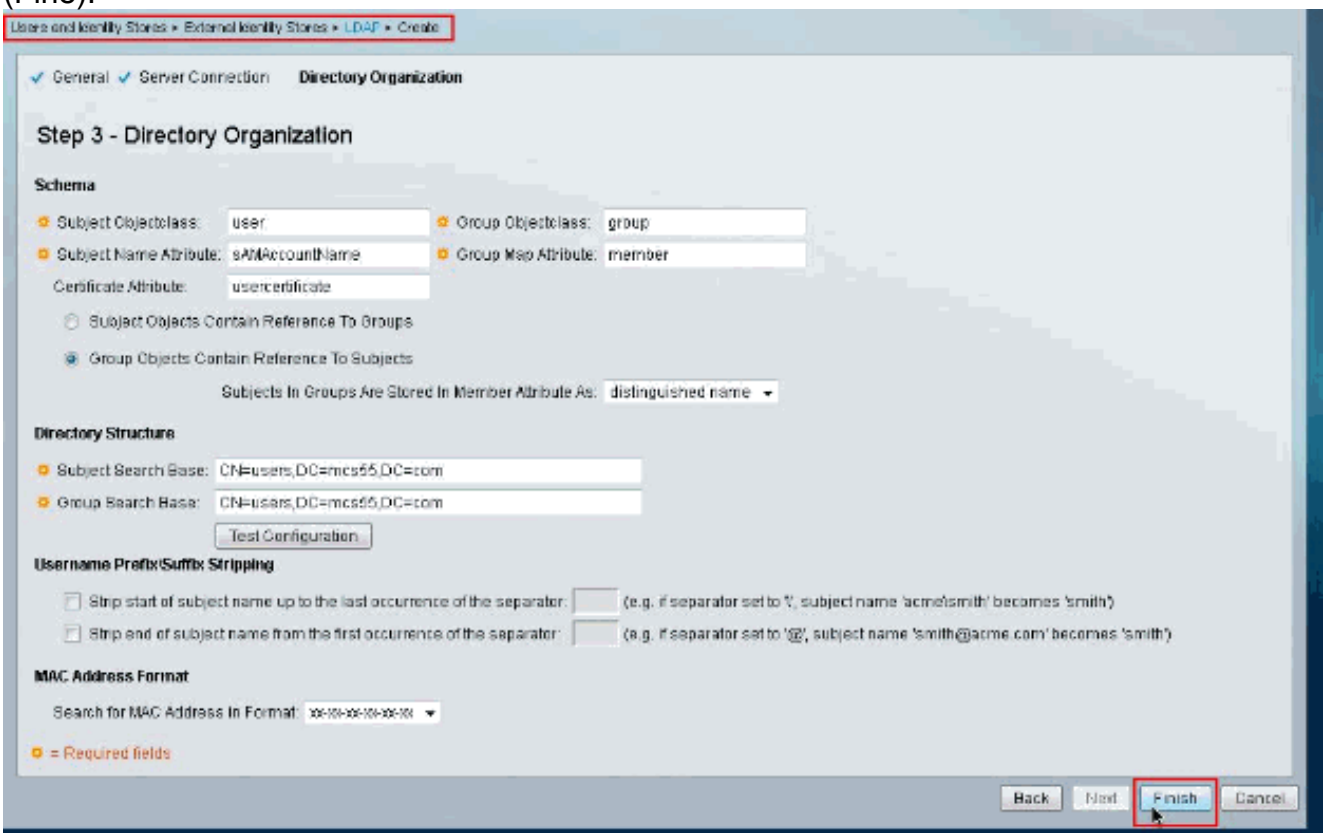
5. Nella scheda **Organizzazione directory** della sezione **Schema** fornire i dettagli necessari. Analogamente, fornire le informazioni richieste nella sezione **Struttura directory** come fornito dall'amministratore LDAP. Fare clic su **Test configurazione**.



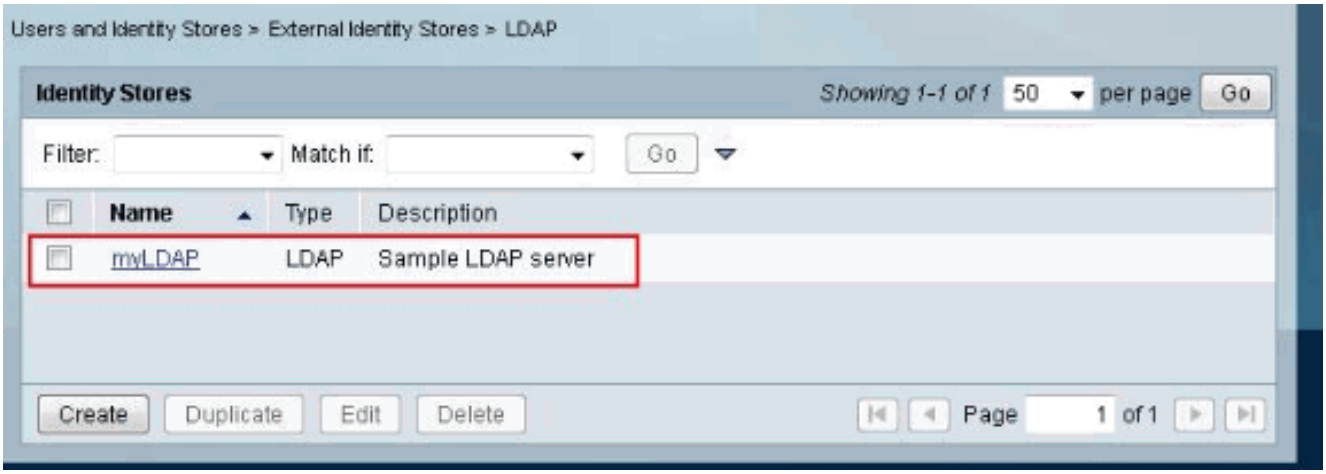
Nell'immagine seguente viene mostrato che il **test di configurazione** è riuscito.**Nota:** se il test Configuration non riesce, verificare nuovamente i parametri forniti nello **schema** e nella **struttura di directory** dall'amministratore LDAP.



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



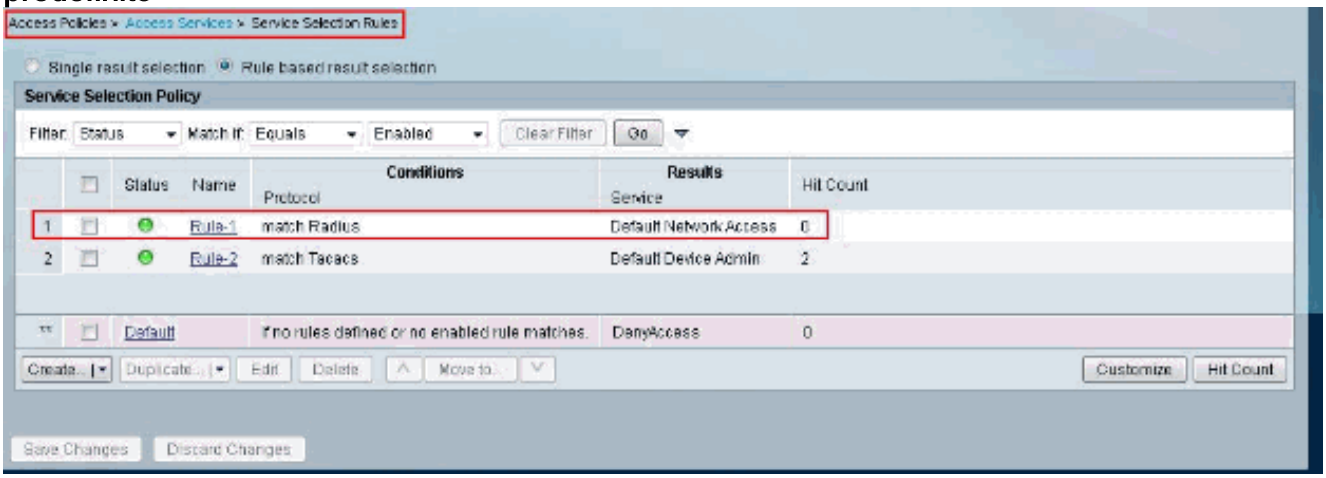
Creazione del **server LDAP** completata.



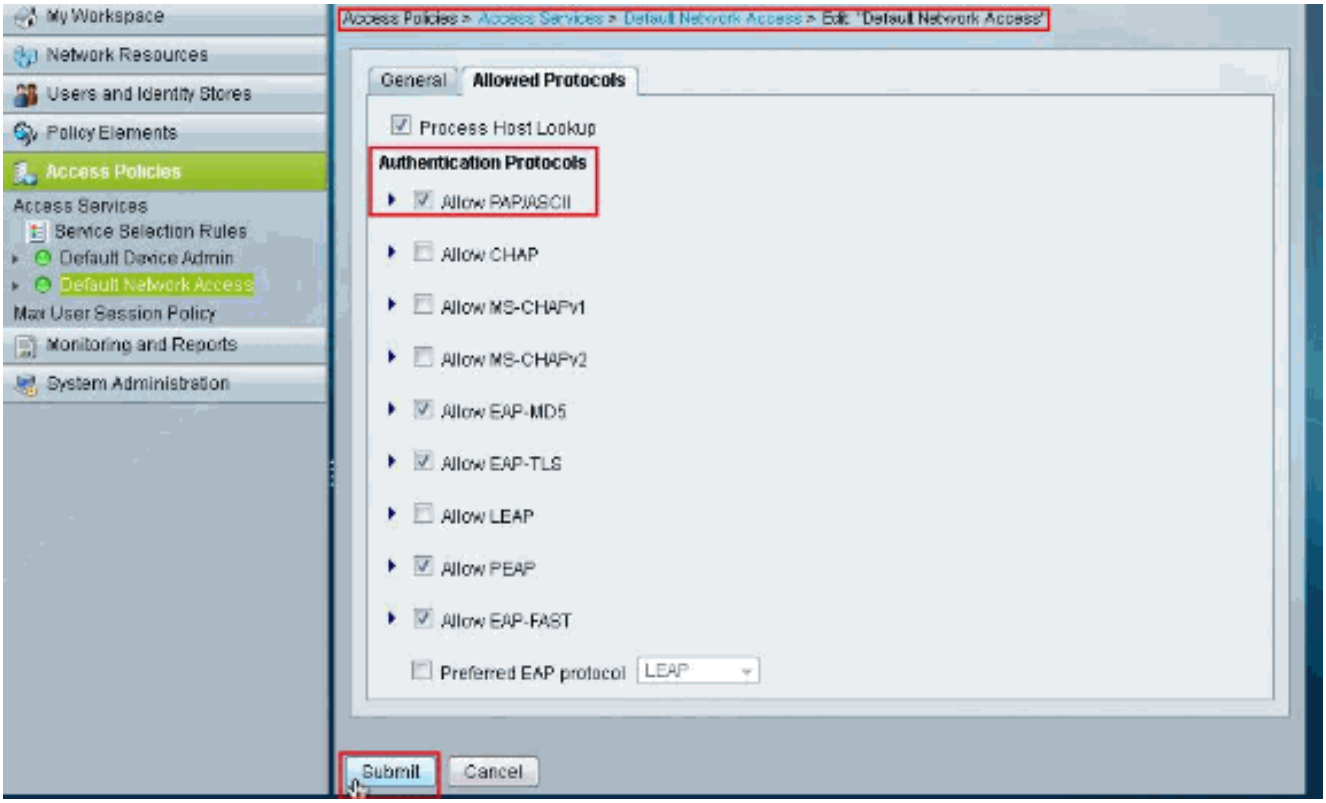
Configura l'archivio identità

Completare questi passaggi per configurare l'archivio identità:

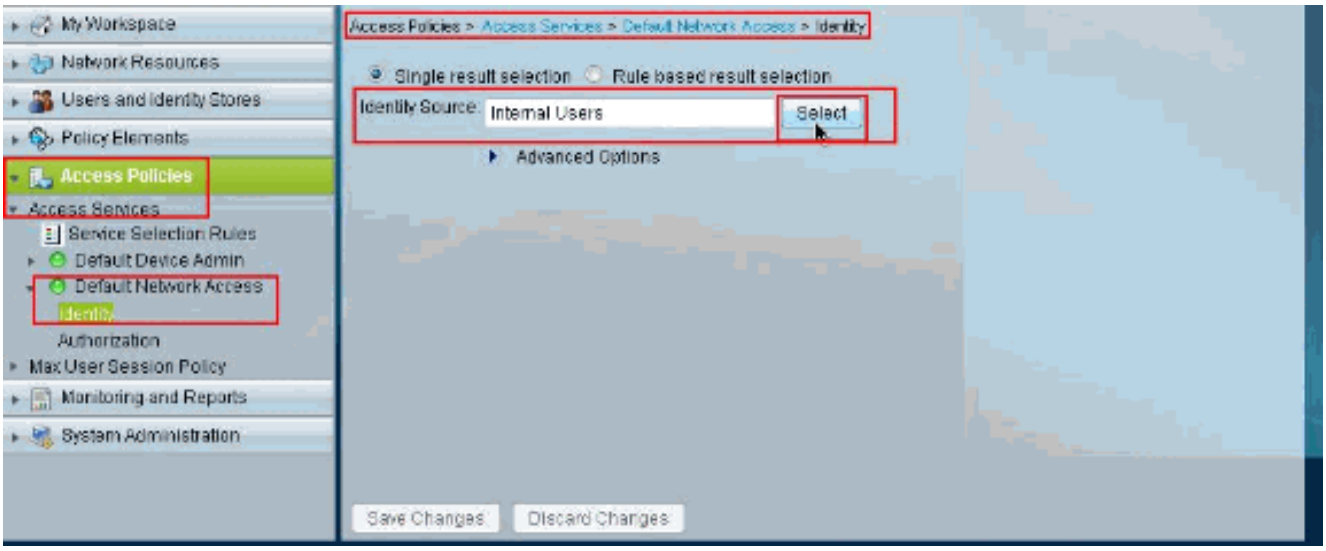
1. Scegliere **Criteri di accesso > Servizi di accesso > Regole selezione servizio** e verificare quale servizio utilizzerà il server LDAP sicuro per l'autenticazione. Nell'esempio il servizio è **Accesso di rete predefinito**.



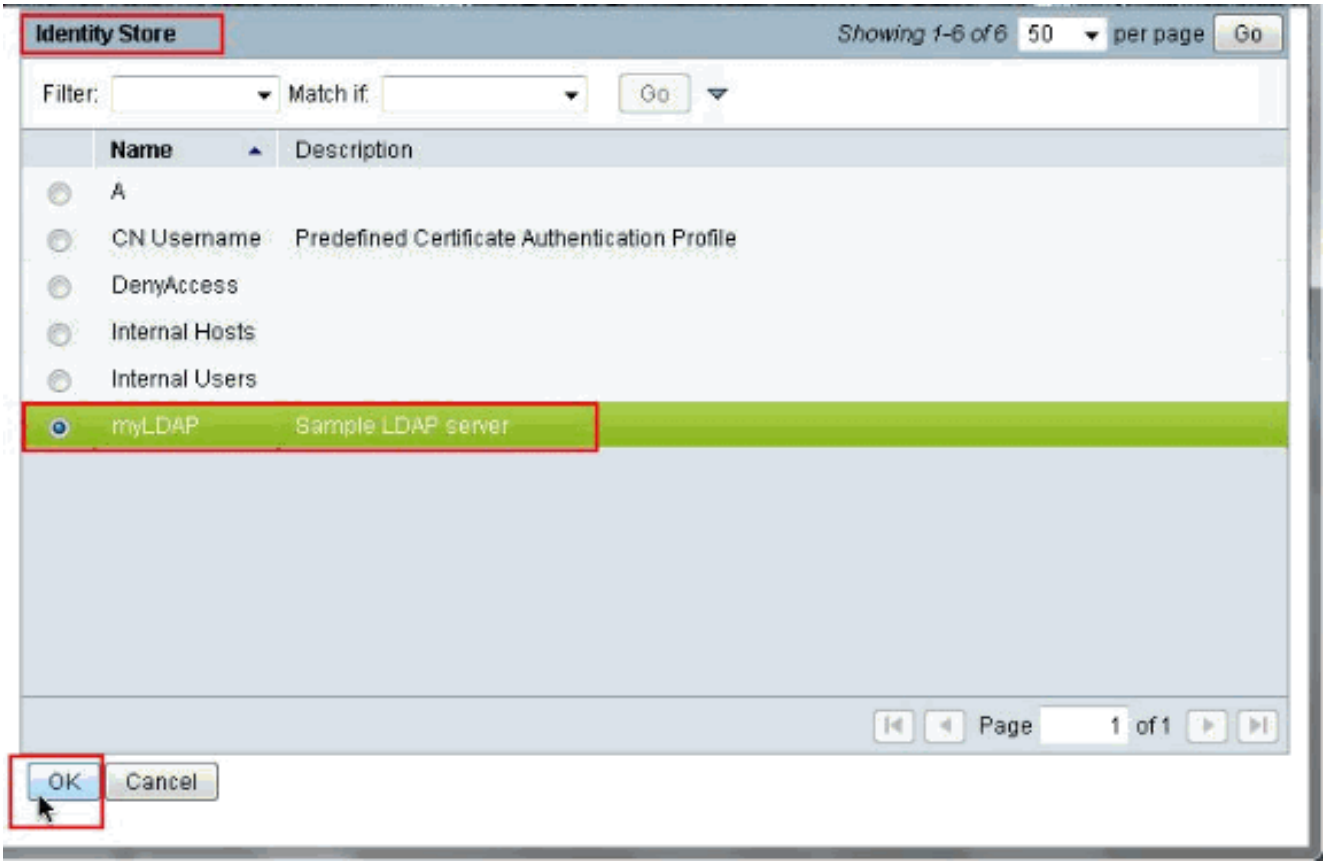
2. Dopo aver verificato il servizio nel passaggio 1, passare al servizio specifico e fare clic su **Protocolli consentiti**. Verificare che l'opzione **Allow PAP/ASCII** sia selezionata, quindi fare clic su **Submit** (Invia).**Nota:** con Consenti PAP/ASCII è possibile selezionare altri protocolli di autenticazione.



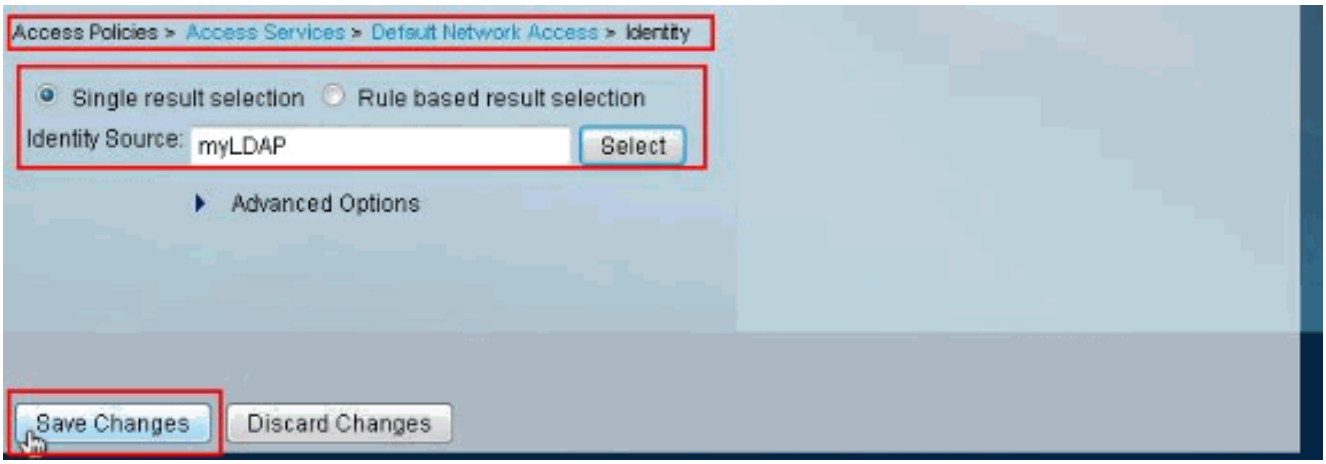
3. Fare clic sul servizio identificato nel passaggio 1, quindi fare clic su **Identità**. Fare clic su **Seleziona** accanto a **Origine identità**.



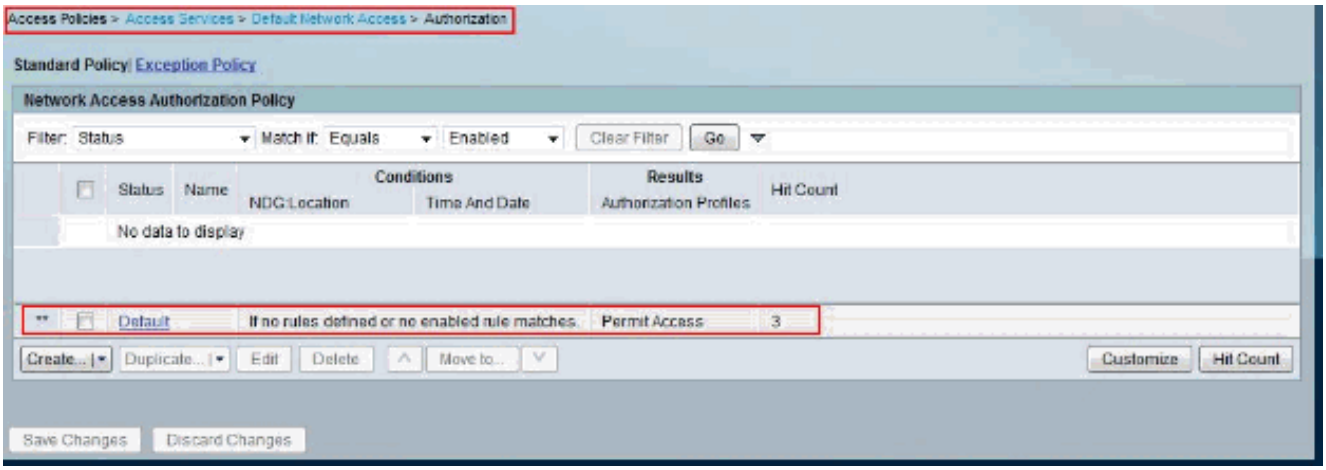
4. Selezionare il **server LDAP sicuro** appena creato (**myLDAP** in questo esempio), quindi fare clic su **OK**.



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 di una risposta da parte di ACS 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**: i possibili motivi per cui un server LDAP restituisce errori di binding (autenticazione) sono: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, il che indica un possibile problema con il server LDAP:

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

Questo errore viene registrato come errore sconosciuto: `Nel database non esiste alcun utente`.

Questo errore viene registrato come errore Password non valida, in cui l'utente esiste, ma la password inviata non è valida: `Password non valida`.

Informazioni correlate

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