

ACS 5.x: Ejemplo de configuración del servidor LDAP

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Servicio de directorio](#)

[Autenticación usando el LDAP](#)

[Administración de la conexión LDAP](#)

[Configurar](#)

[Configuración ACS 5.x para el LDAP](#)

[Configure el almacén de la identidad](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

El Lightweight Directory Access Protocol (LDAP) es un Networking Protocol para los servicios de directorio que preguntan y de modificaciones que se ejecutan en el TCP/IP y el UDP. LDAP es un mecanismo ligero para acceder a un servidor de directorio basado en x.500. [RFC 2251 define LDAP.](#)

El Cisco Secure Access Control System (ACS) 5.x integra con una base de datos externa LDAP (también llamada un almacén de la identidad) usando el protocolo LDAP. Hay dos métodos usados para conectar con el servidor LDAP: sólo texto (simple) y conexión SSL (cifrado). El ACS 5.x se puede configurar para conectar con el servidor LDAP que usa ambos métodos. Este documento proporciona un ejemplo de configuración para conectar ACS 5.x con un servidor LDAP usando una conexión simple.

[prerrequisitos](#)

[Requisitos](#)

Este documento asume que el ACS 5.x tiene una conexión IP al servidor LDAP y que el puerto TCP 389 está abierto.

Por abandono, configuran al servidor LDAP del Microsoft Active Directory para validar las

conexiones LDAP en el puerto TCP 389. Si usted está utilizando a cualquier otro servidor LDAP, asegúrese que es en servicio y que valida las conexiones en el puerto TCP 389.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure ACS 5.x
- Servidor LDAP del Microsoft Active Directory

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

Antecedentes

Servicio de directorio

El servicio de directorio es una aplicación de software o un conjunto de las aplicaciones usadas para salvar y para ordenar la información sobre los usuarios y los recursos de red de una red informática. Usted puede utilizar el servicio de directorio para manejar el acceso del usuario a estos recursos.

El servicio de directorio LDAP se basa en un client-server model. Un cliente conecta con un servidor LDAP para comenzar una sesión LDAP, y envía las peticiones de la operación al servidor. El servidor entonces envía sus respuestas. Uno o más servidores LDAP contienen los datos del árbol de directorio LDAP o de la base de datos del back-end LDAP.

El servicio de directorio maneja el directorio, que es la base de datos que lleva a cabo la información. Los servicios de directorio utilizan un modelo distribuido para salvar la información, y esa información se replica generalmente entre los Servidores del directorio.

Un directorio LDAP se ordena en una jerarquía de árbol simple y se puede distribuir entre muchos servidores. Cada servidor puede tener una versión replicada del directorio total que se sincroniza periódicamente.

Una entrada en el árbol contiene un conjunto de los atributos, donde cada atributo tiene un nombre (un tipo del atributo o una descripción del atributo) y uno o más valores. Los atributos se definen en un esquema.

Cada entrada tiene un Identificador único llamado su Nombre distintivo (DN). Este nombre contiene el nombre distintivo relativo (RDN) construido de los atributos en la entrada, seguida por el DN de la entrada del padre. Usted puede pensar en el DN como nombre de fichero completo, y el RDN como nombre de fichero relativo en una carpeta.

[Autenticación usando el LDAP](#)

El ACS 5.x puede autenticar un principal contra un almacén de la identidad LDAP realizando una operación del lazo en el Servidor del directorio para encontrar y autenticar el principal. Si la autenticación tiene éxito, el ACS puede extraer los grupos y los atributos que pertenecen al principal. Los atributos a extraer se pueden configurar en la interfaz Web ACS (páginas LDAP). Estos grupos y atributos pueden ser utilizados por el ACS para autorizar el principal.

Para autenticar a un usuario o preguntar el almacén de la identidad LDAP, el ACS conecta con el servidor LDAP y mantiene un pool de la conexión. Vea la [Administración de la conexión LDAP](#).

[Administración de la conexión LDAP](#)

El ACS 5.x soporta las conexiones LDAP simultáneas múltiples. Las conexiones se abren a pedido a la hora de la primera autenticación ldap. La cantidad máxima de conexiones se configura para cada servidor LDAP. La apertura de las conexiones acorta por adelantado el tiempo de la autenticación.

Usted puede fijar la cantidad máxima de conexiones para utilizar para las conexiones obligatorias simultáneas. El número de conexiones abiertas puede ser diferente para cada servidor LDAP (primario o secundario) y se determina según el número máximo de conexiones de la administración configuradas para cada servidor.

El ACS conserva una lista de conexiones LDAP abiertas (información incluyendo del lazo) para cada servidor LDAP que se configure en el ACS. Durante el proceso de autenticación, el administrador de conexión intenta encontrar una conexión abierta del pool.

Si no existe una conexión abierta, se abre un nuevo. Si el servidor LDAP cerró la conexión, el administrador de conexión señala un error durante la primera llamada para buscar el directorio, e intenta renovar la conexión.

Después de que el proceso de autenticación sea completo, el administrador de conexión libera la conexión al administrador de conexión. Para más información, refiera al [guía del usuario ACS 5.X](#).

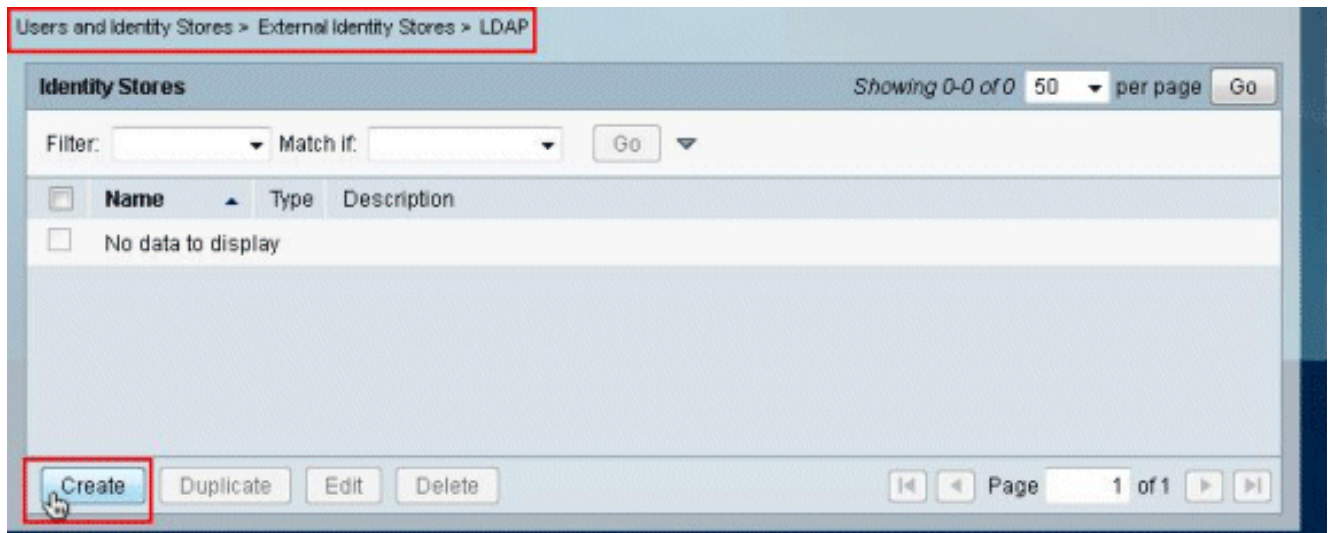
[Configurar](#)

En esta sección encontrará la información para configurar las funciones descritas en este documento.

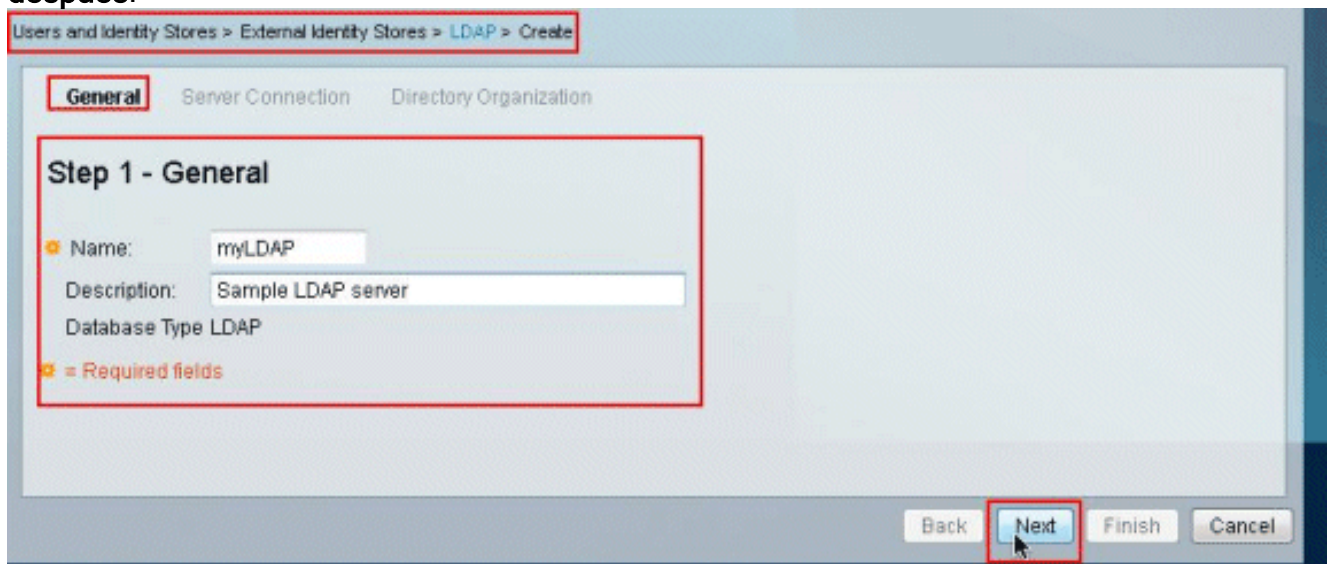
[Configuración ACS 5.x para el LDAP](#)

Complete estos pasos para configurar ACS 5.x para el LDAP:

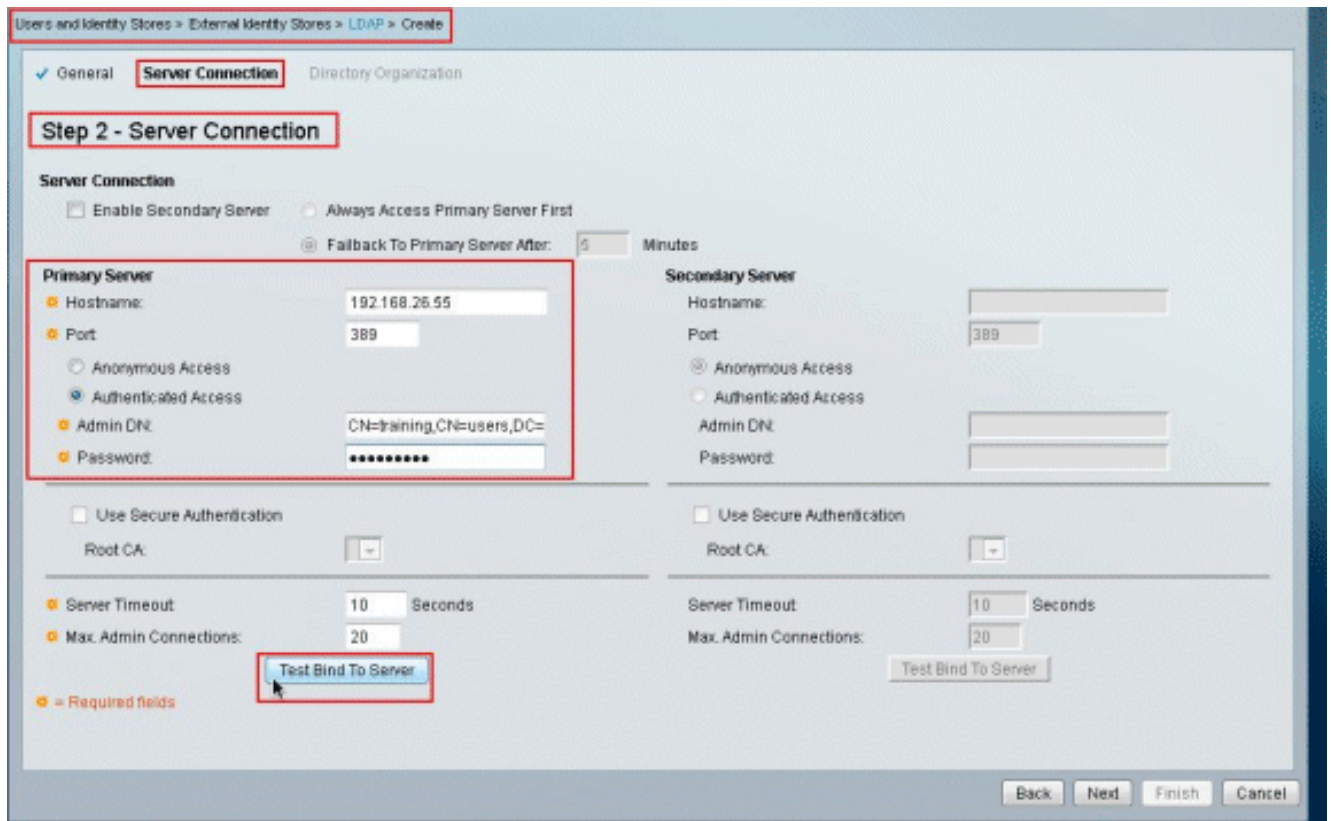
1. Elija a los **usuarios y la identidad salva > identidad externa salva > LDAP**, y el teclado crea para crear una nueva conexión LDAP.



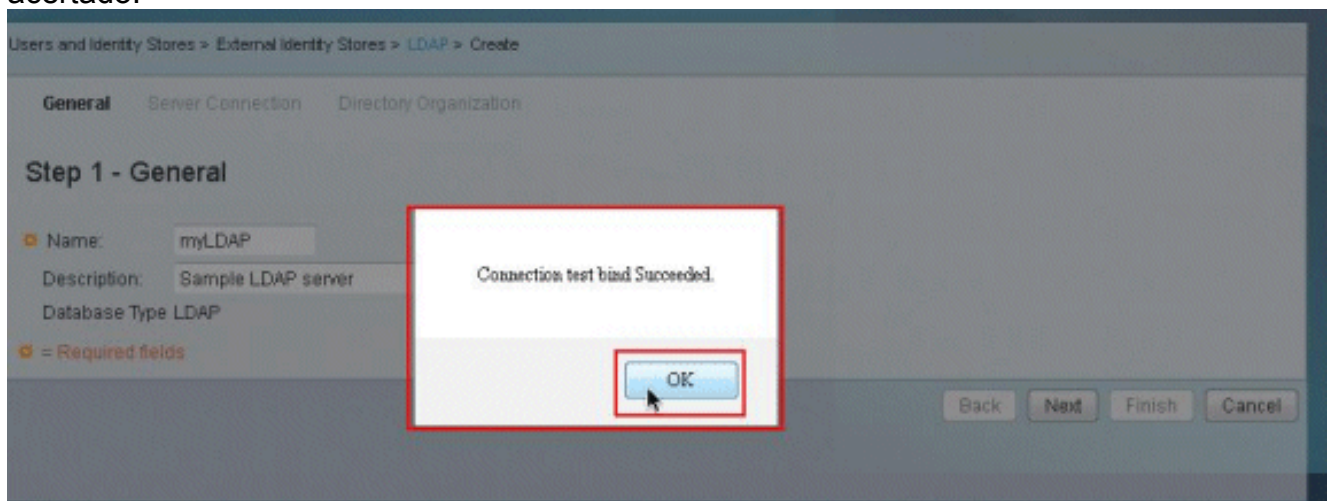
2. En la ficha general, proporcione el **nombre** y la **descripción** (opcionales) para el nuevo LDAP, y haga clic **después**.



3. En la lengüeta de la conexión del servidor bajo sección del servidor primario, proporcione el **nombre de host**, el **puerto**, el **Admin DN**, y la **contraseña**. Haga clic el **lazo de la prueba al servidor**. **Nota:** El número del puerto asignado IANA para el LDAP es TCP 389. Sin embargo, confirme el número del puerto que su servidor LDAP está utilizando de su LDAP Admin. El Admin DN y contraseña se debe proporcionarle por su LDAP Admin. Su Admin DN debe haber leído todos los permisos en todos los OU en el servidor LDAP.

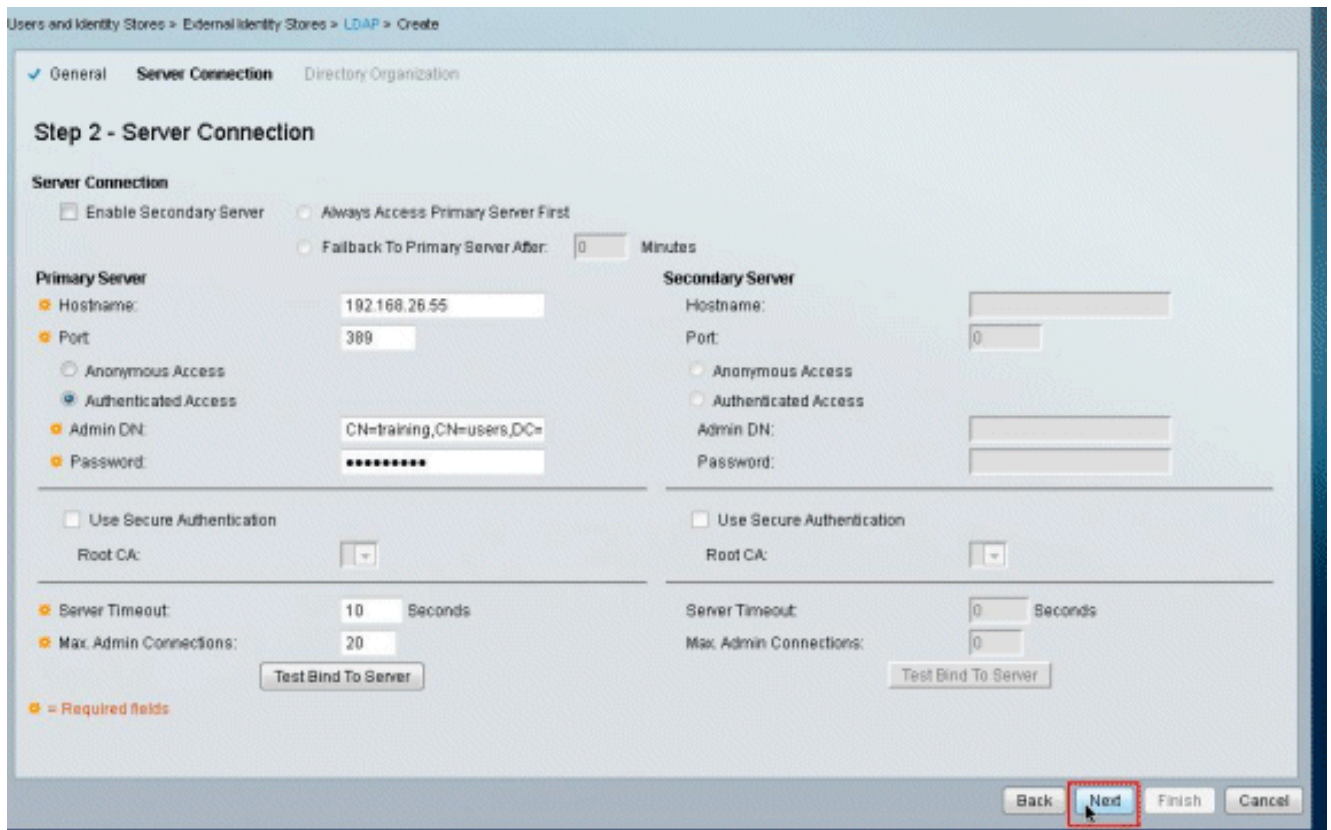


4. Esta imagen muestra que el lazo de la prueba de la conexión al servidor era acertado.

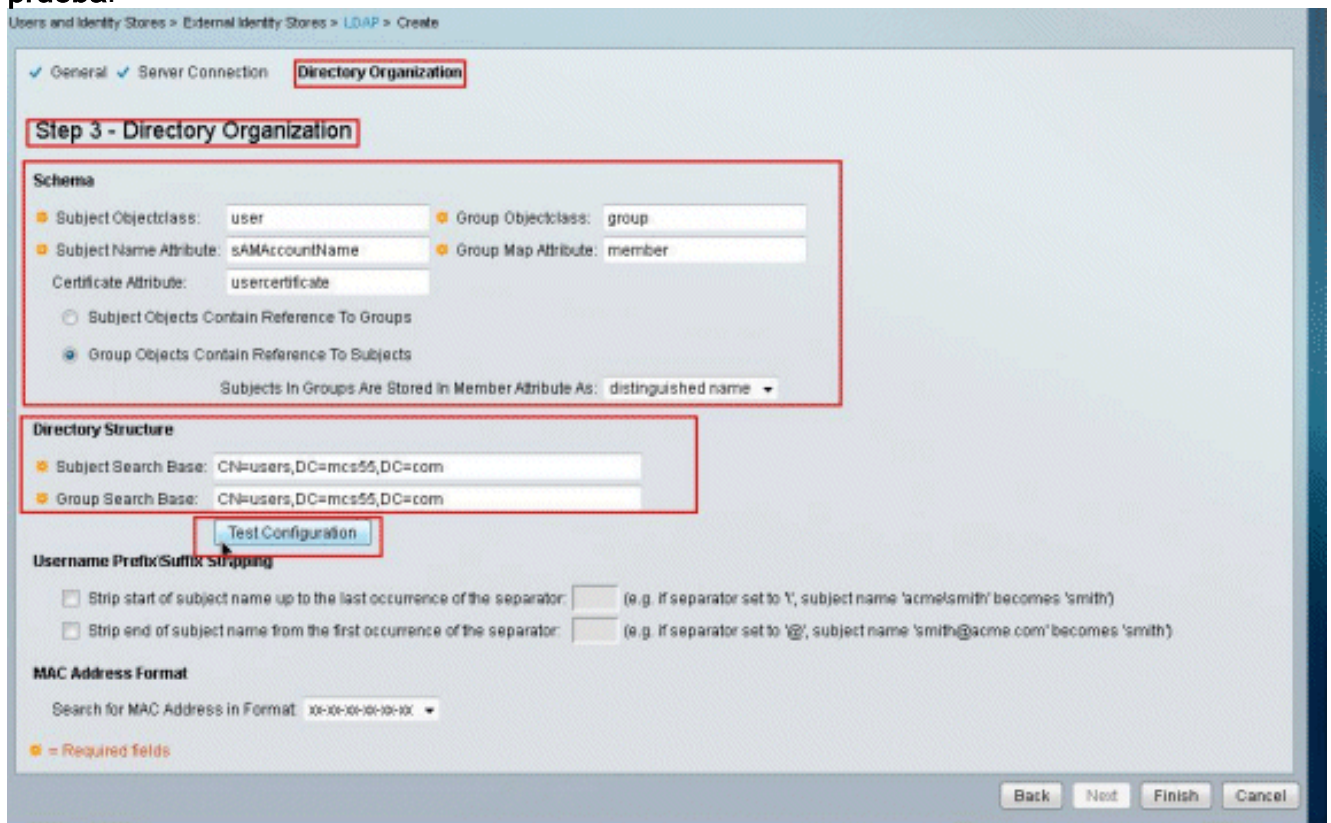


Nota: Si el lazo de la prueba no es acertado, re-verifique el nombre de host, el número del puerto, el Admin DN, y la contraseña de su administrador LDAP.

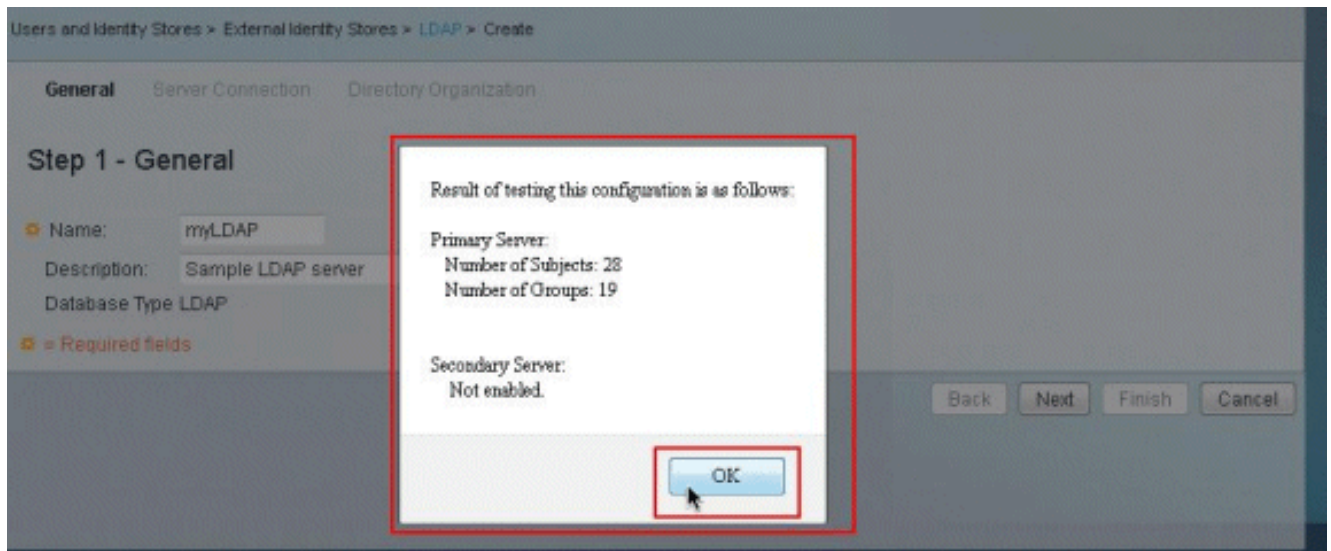
5. Haga clic en Next (Siguiete).



6. Proporcione los detalles requeridos en la lengüeta de la organización del directorio bajo sección del esquema. Semejantemente, proporcione la Información requerida bajo sección de la estructura de directorios como está previsto por su LDAP Admin. Haga clic la configuración de la prueba.

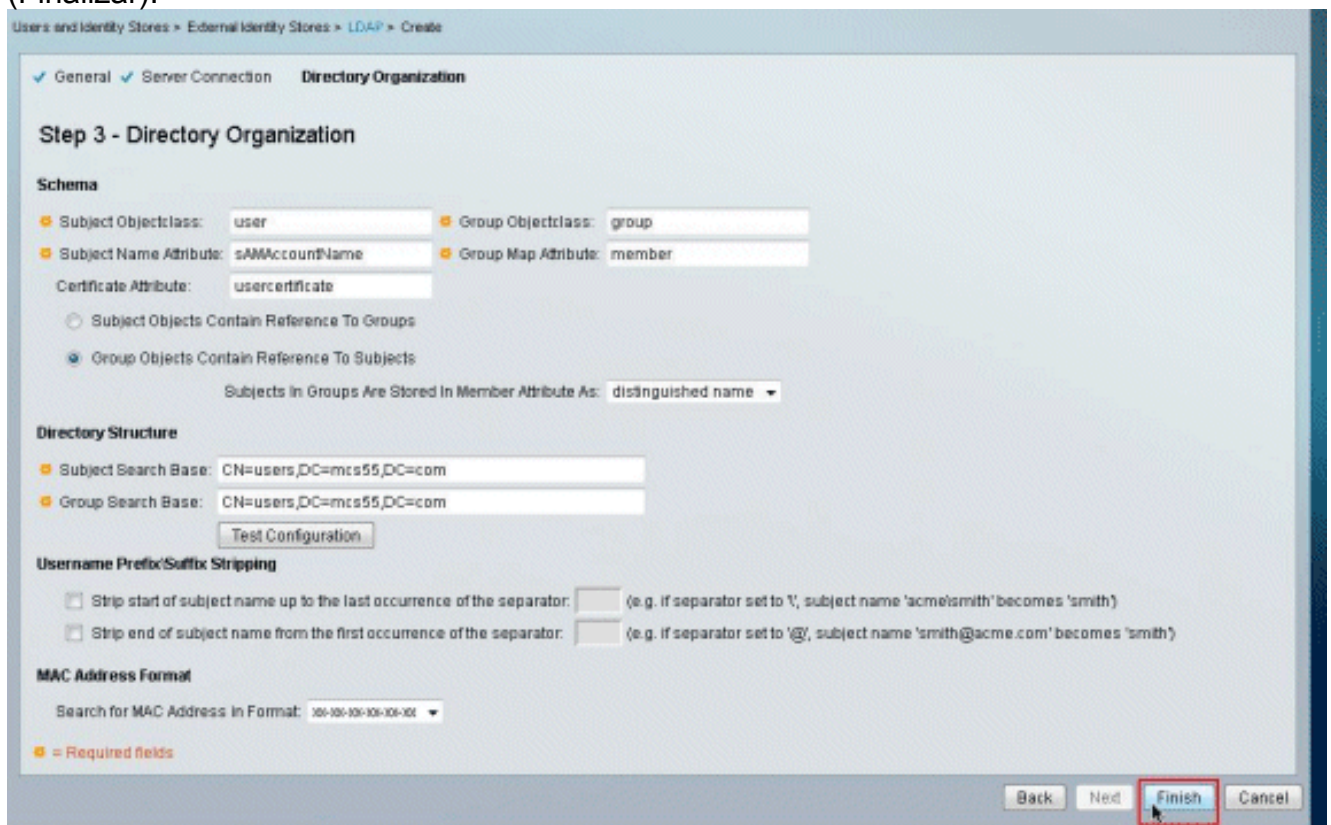


7. Esta imagen muestra que la prueba de la configuración es acertada.

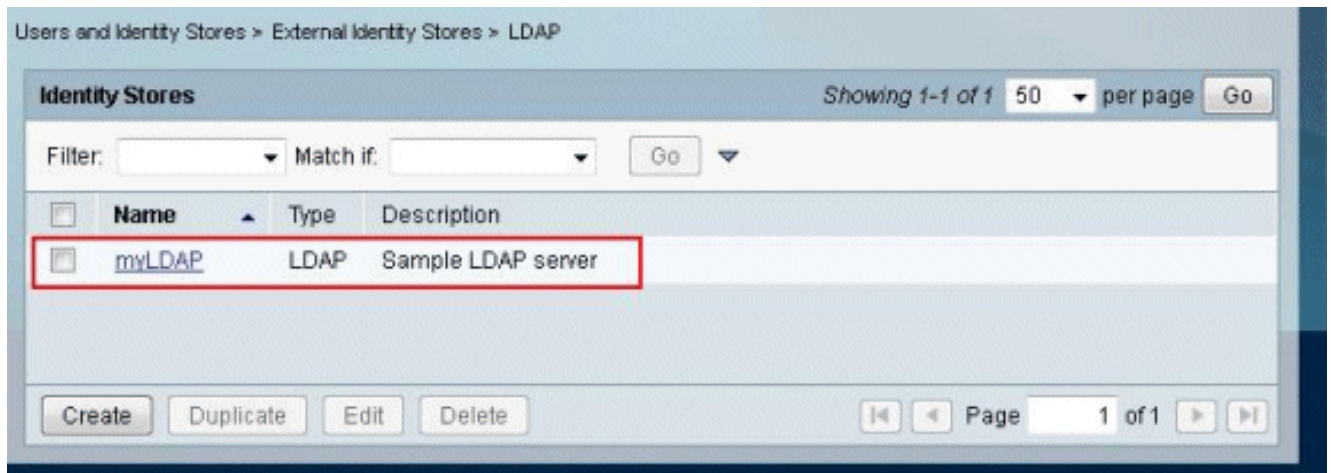


Nota: Si la prueba de la configuración no es acertada, re-verifique los parámetros proporcionados en el **esquema** y la **estructura de directorios** de su administrador LDAP.

8. Haga clic en Finish (Finalizar).



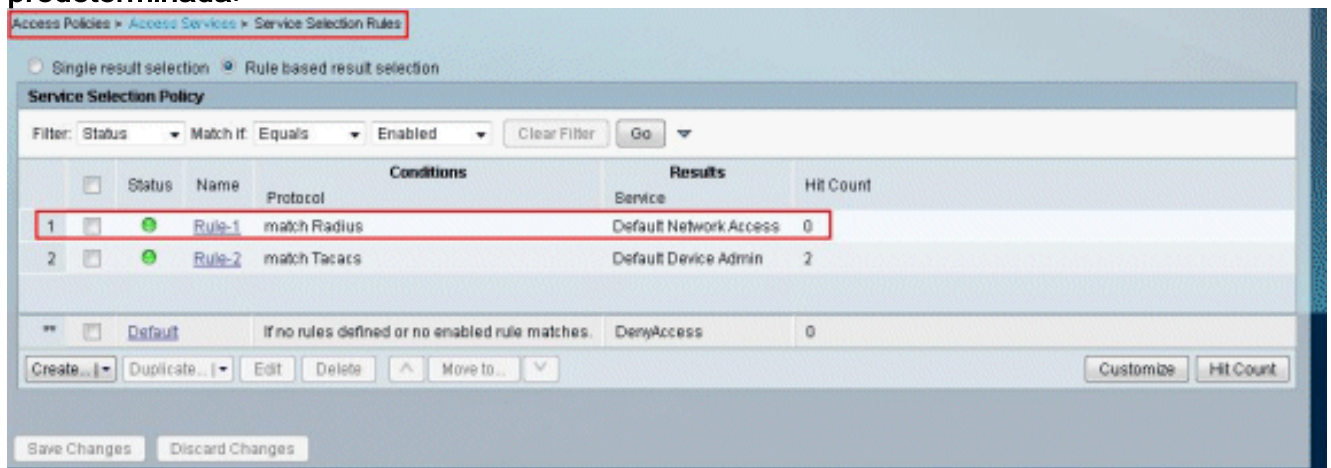
9. Crean al **servidor LDAP** con éxito.



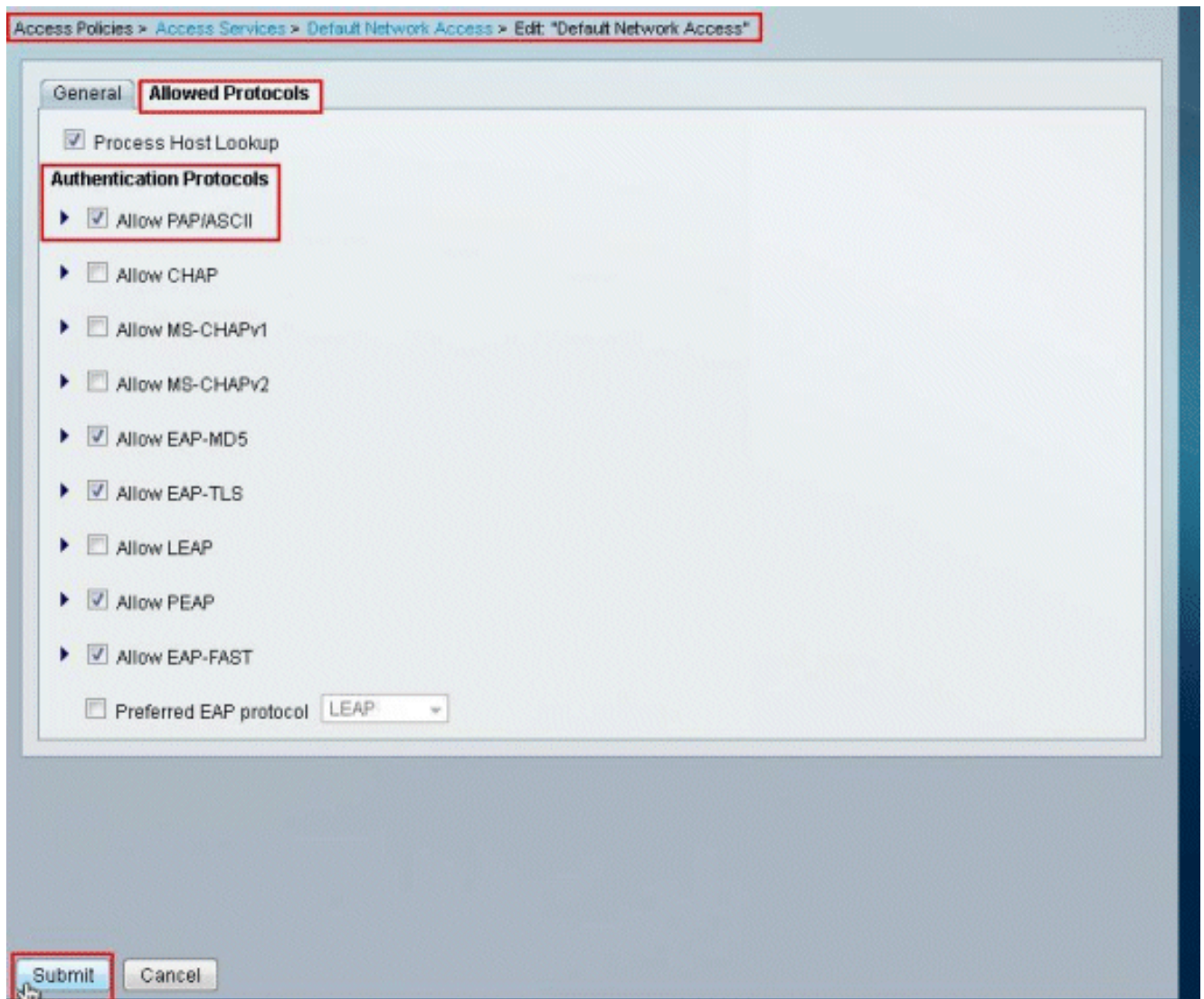
[Configure el almacén de la identidad](#)

Compien los pasos para configurar el almacén de la identidad:

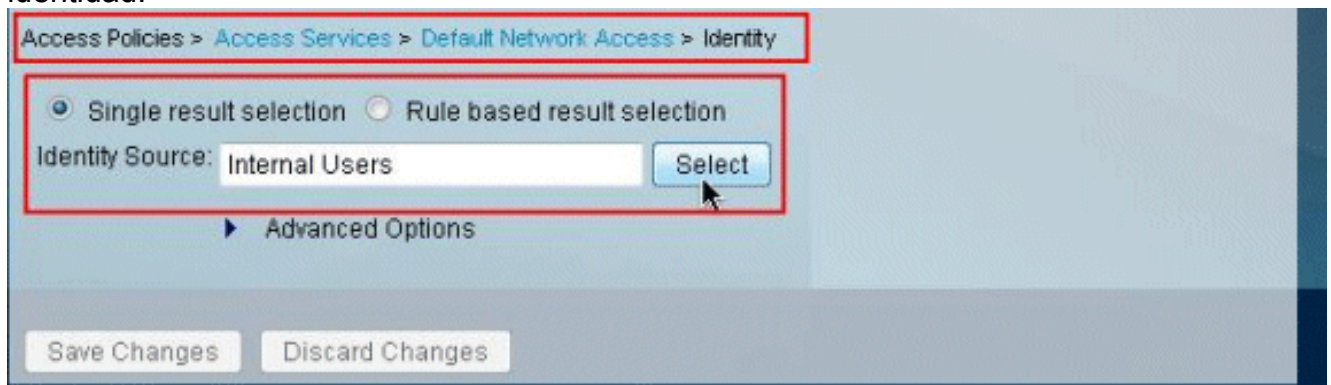
1. Elija las **políticas de acceso** > el **acceso mantiene** > las **reglas de selección del servicio**, y verifica qué servicio va a utilizar al servidor LDAP para la autenticación. En este ejemplo, la autenticación de servidor LDAP utiliza el servicio del **acceso de red predeterminada**.



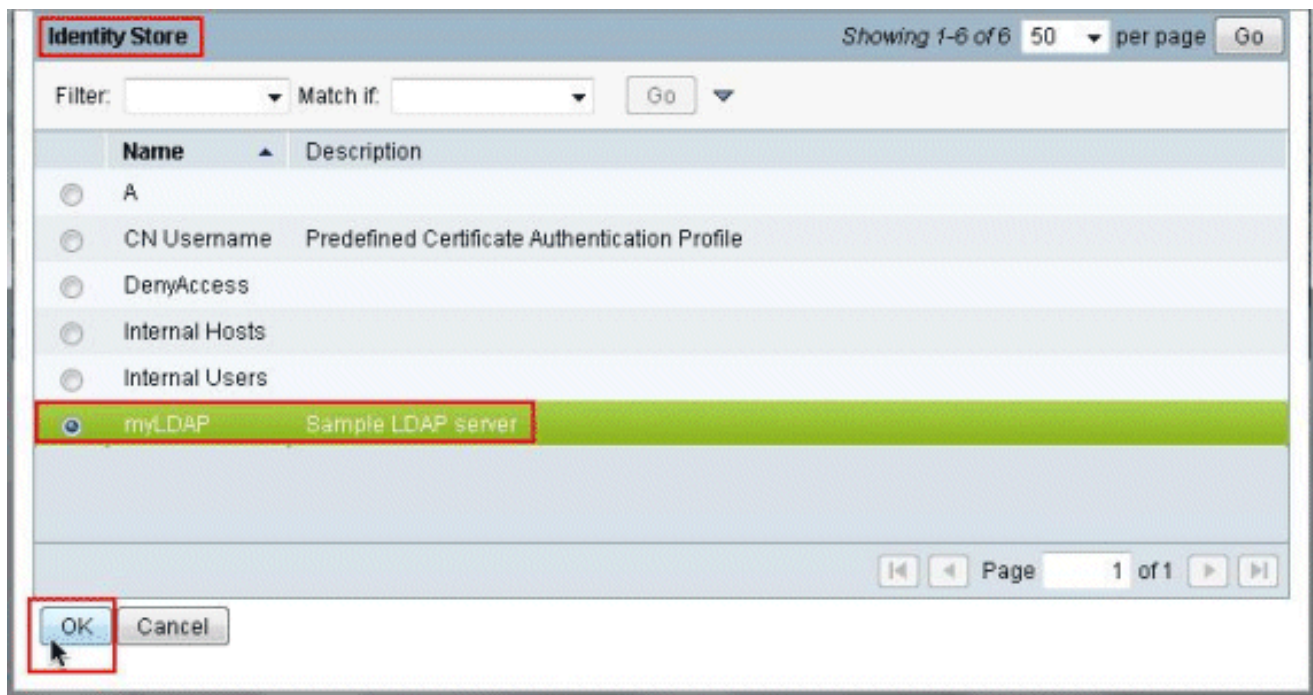
2. Una vez que usted ha verificado el servicio en el paso 1, vaya al servicio determinado y haga clic los **protocolos permitidos**. Asegurese que **permite PAP/ASCII** está seleccionado, y el tecleo **somete**. **Nota:** Usted puede tener otros Protocolos de autenticación seleccionados junto con para permitir PAP/ASCII.



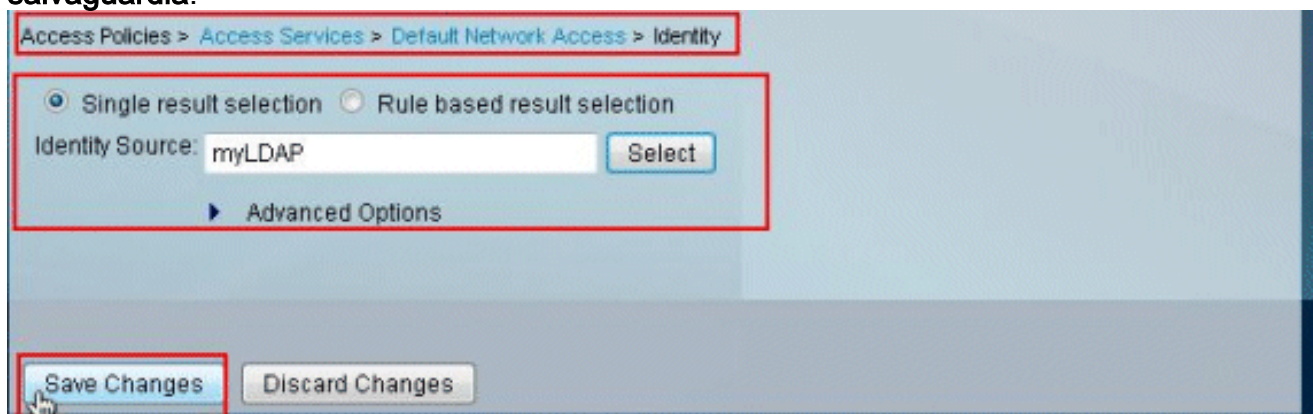
3. Haga clic en el servicio identificado en el paso 1, y haga clic la **identidad**. Haga clic **selecto** a la derecha del campo de fuente de la identidad.



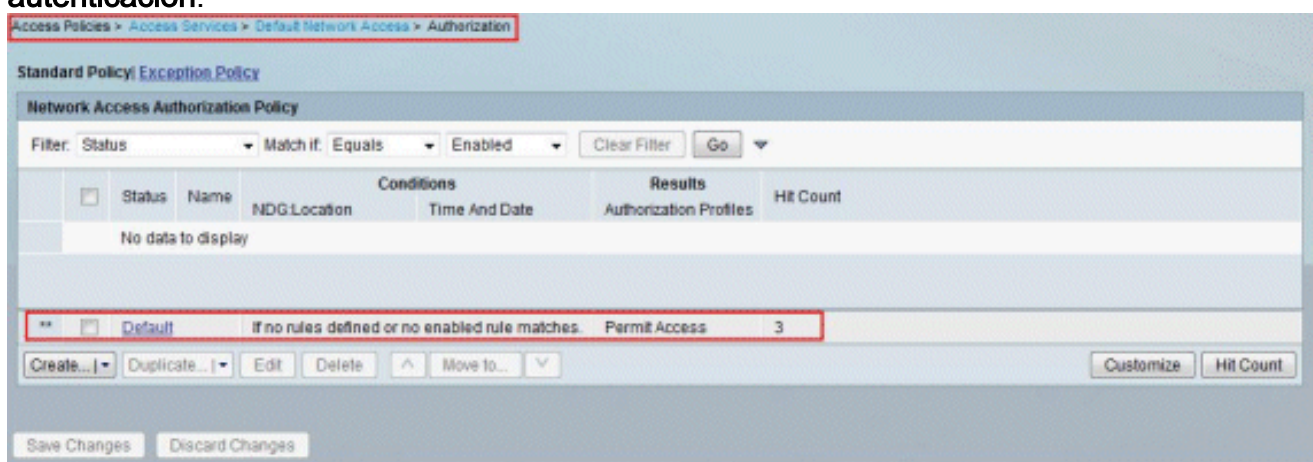
4. Seleccione al servidor LDAP creado recientemente (**myLDAP**, en este ejemplo), y haga clic la **AUTORIZACIÓN**.



5. Haga clic los cambios de la salvaguardia.



6. Vaya a la sección de la autorización del servicio identificado en el paso 1, y asegurese que hay por lo menos una regla que permite la autenticación.



Troubleshooting

El ACS envía una petición del lazo de autenticar al usuario contra un servidor LDAP. La petición del lazo contiene el DN y la contraseña del usuario del usuario en el texto claro. Autentican a un

usuario cuando el DN y las coincidencias de contraseña del usuario el nombre de usuario y contraseña en el directorio LDAP.

- **Errores de autenticación** - El ACS registra los errores de autenticación en los archivos del registro ACS.
- **Errores de inicialización** - Utilice las configuraciones de tiempo de espera del servidor LDAP para configurar el número de segundos que el ACS espere una respuesta de un servidor LDAP antes de determinar eso la conexión o la autenticación en ese servidor ha fallado. Las razones posibles de un servidor LDAP para volver un error de inicialización son:El LDAP no se soportaEl servidor está abajoEl servidor está fuera de memoriaEl usuario no tiene ningún privilegioSe configuran las credenciales incorrectas del administrador
- **Errores del lazo** - Las razones posibles de un servidor LDAP para volver los errores del lazo (autenticación) son:Errores de filtraciónUna búsqueda usando los criterios del filtro fallaErrores del parámetroLos parámetros inválidos fueron ingresadosLa cuenta de usuario es restringida (inhabilitado, bloqueado hacia fuera, expirado, la contraseña expiró, y así sucesivamente)

Estos errores se registran como errores del recurso externo, indicando un Posible problema con el servidor LDAP:

- Un error de conexión ocurrió
- El descanso expiró
- El servidor está abajo
- El servidor está fuera de memoria

El usuario A no existe en el error en la base de datos se registra como error del usuario desconocido.

Una contraseña no válida era error ingresado se registra como error de la contraseña no válida, donde existe el usuario, pero la contraseña enviada es inválida.

[Información Relacionada](#)

- [Cisco Secure Access Control System](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)