ACS 5.X: Asegure el ejemplo de configuración del servidor LDAP

Contenido

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 Access Control Server (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 a 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 los métodos. En este documento el ACS 5.x se configura para conectar con un servidor LDAP que usa la conexión encriptada.

prerrequisitos

Requisitos

Este documento asume que el ACS 5.x tiene una conexión IP al servidor LDAP y el puerto TCP 636 está abierto.

El servidor LDAP del Active Directory del Microsoft® necesita ser configurado para validar asegura las conexiones LDAP en el puerto TCP 636. Este documento asume que usted tiene el certificado raíz del Certification Authority (CA) que publicó el certificado de servidor al servidor LDAP de Microsoft. Para más información sobre cómo configurar al servidor LDAP, refiérase a cómo habilitar el LDAP sobre el SSL con las autoridades de certificación de tercera persona.

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, para la información que salva y de ordenación 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 comienza una sesión LDAP conectando con un servidor 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: 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 para 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.

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

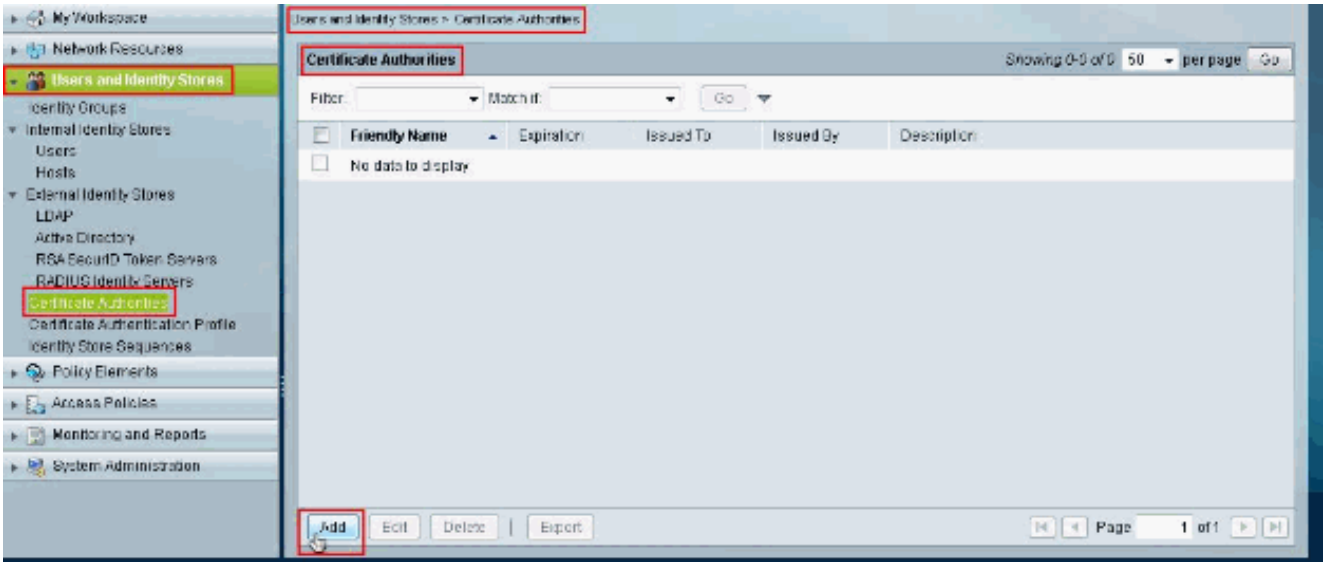
En esta sección encontrará la información para configurar las funciones descritas en este documento.

Instale certificado raíz CA en ACS 5.x

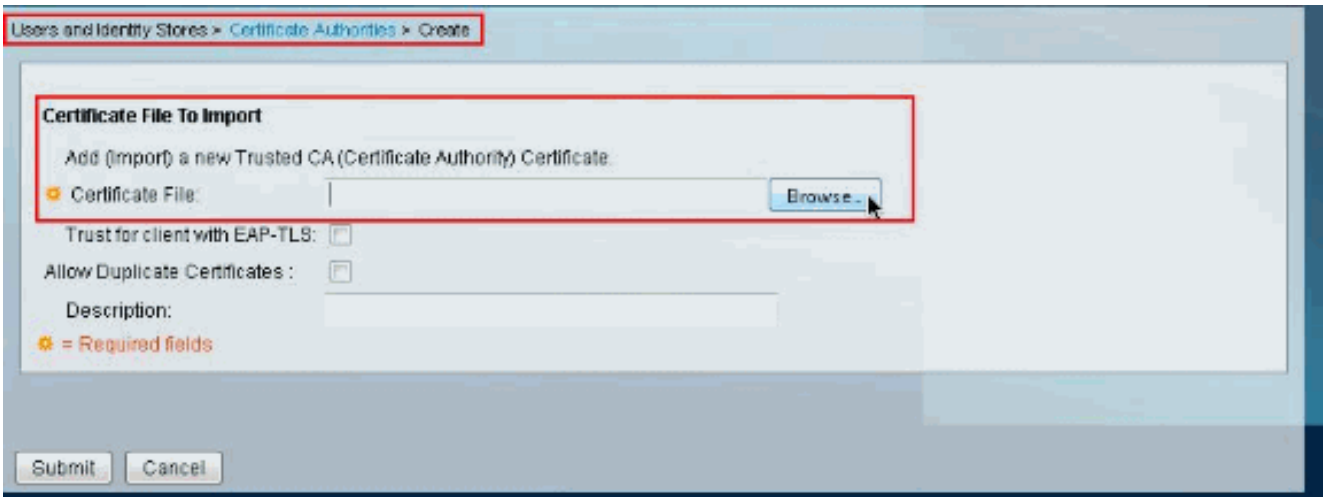
Complete estos pasos para instalar a certificado raíz CA en el Cisco Secure ACS 5.x:

Nota: Asegúrese de que preconfiguren al servidor LDAP para validar las conexiones encriptadas en el puerto TCP 636. Para más información sobre cómo configurar al servidor LDAP de Microsoft, refiérase a cómo habilitar el LDAP sobre el SSL con las autoridades de certificación de tercera persona.

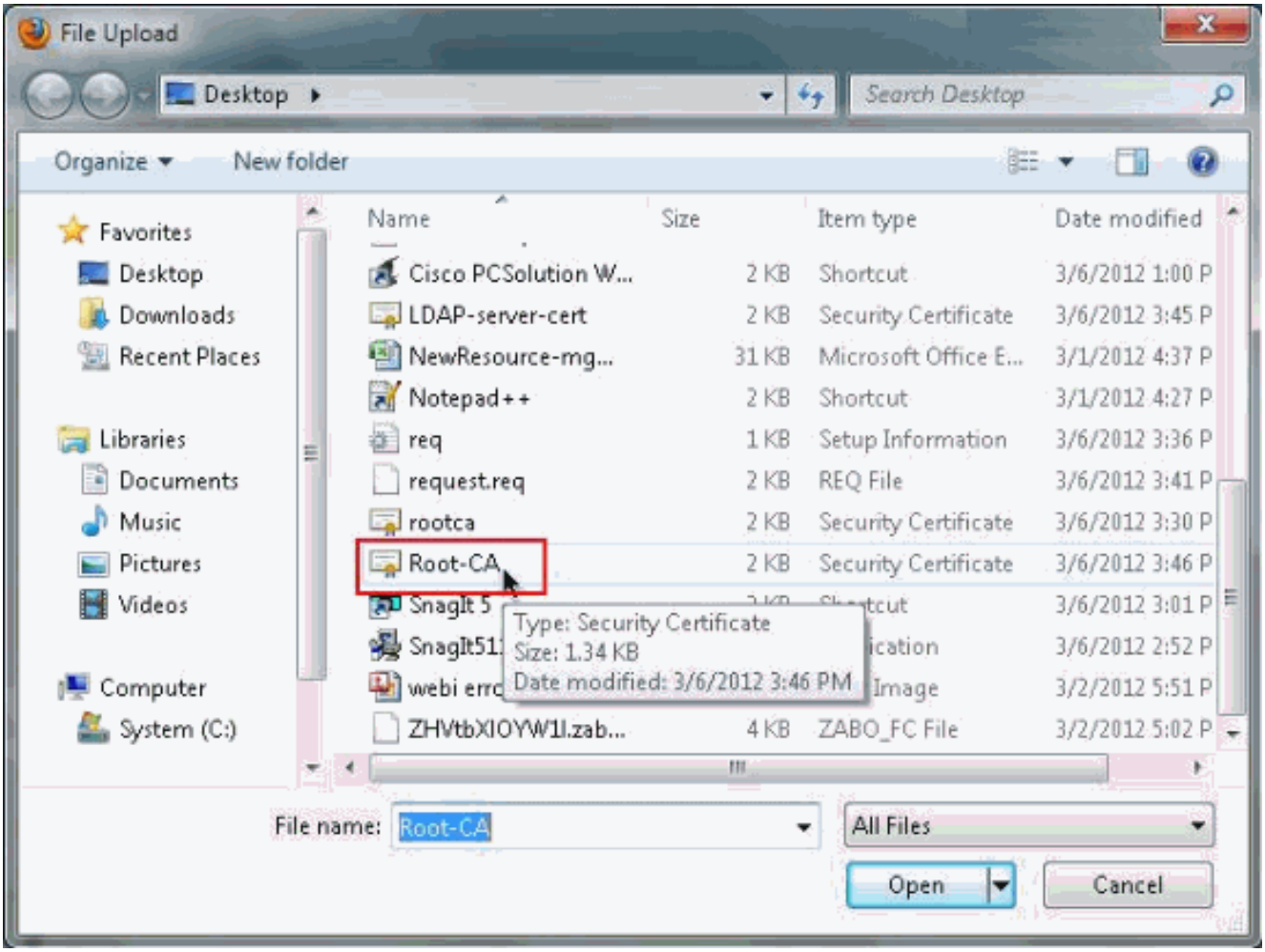
1. Elija a los **usuarios y la identidad salva** > las **autoridades de certificación**, después hace clic **agrega** para agregar el certificado raíz de CA que publicó el certificado de servidor al servidor LDAP de
   Microsoft.



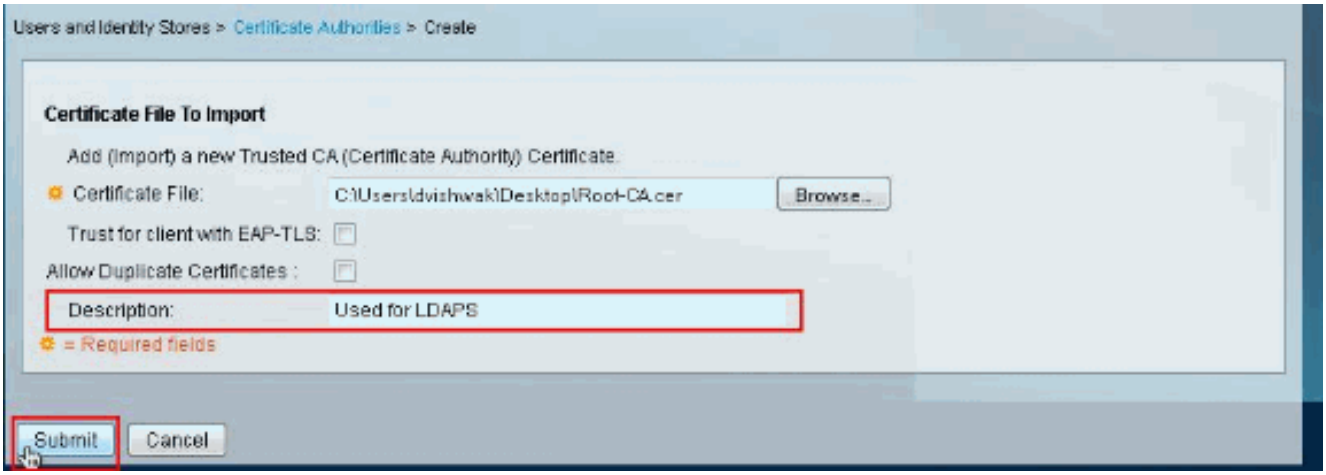
2. **Del archivo de certificado para importar la** sección, el tecleo **hojea** al lado del **archivo de certificado** para buscar para el archivo de certificado.



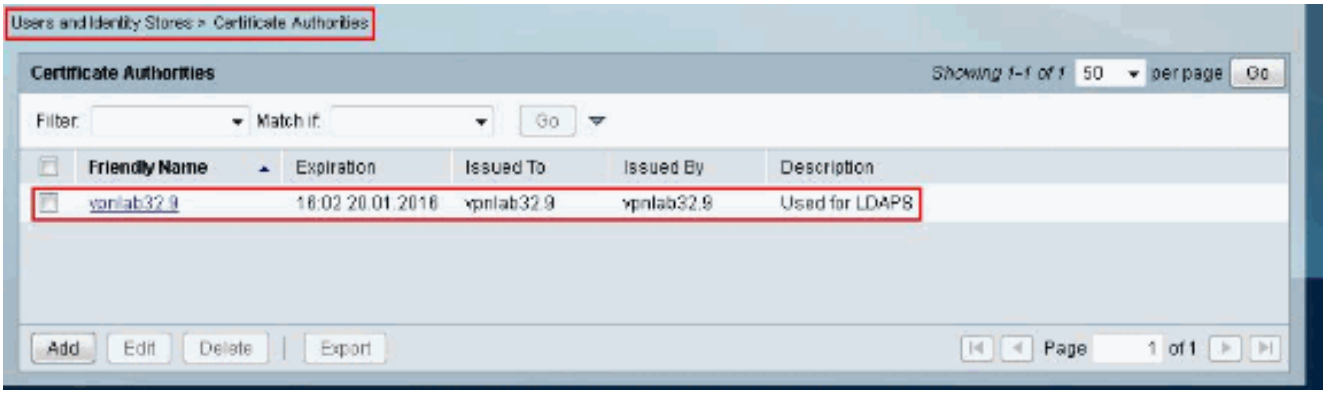
3. Elija el **archivo de certificado** requerido (el certificado raíz de CA que publicó el certificado de servidor al servidor LDAP de Microsoft) y haga clic **abierto**.



4. Proporcione una **descripción** en el espacio proporcionado al lado de la descripción y el tecleo
somete.



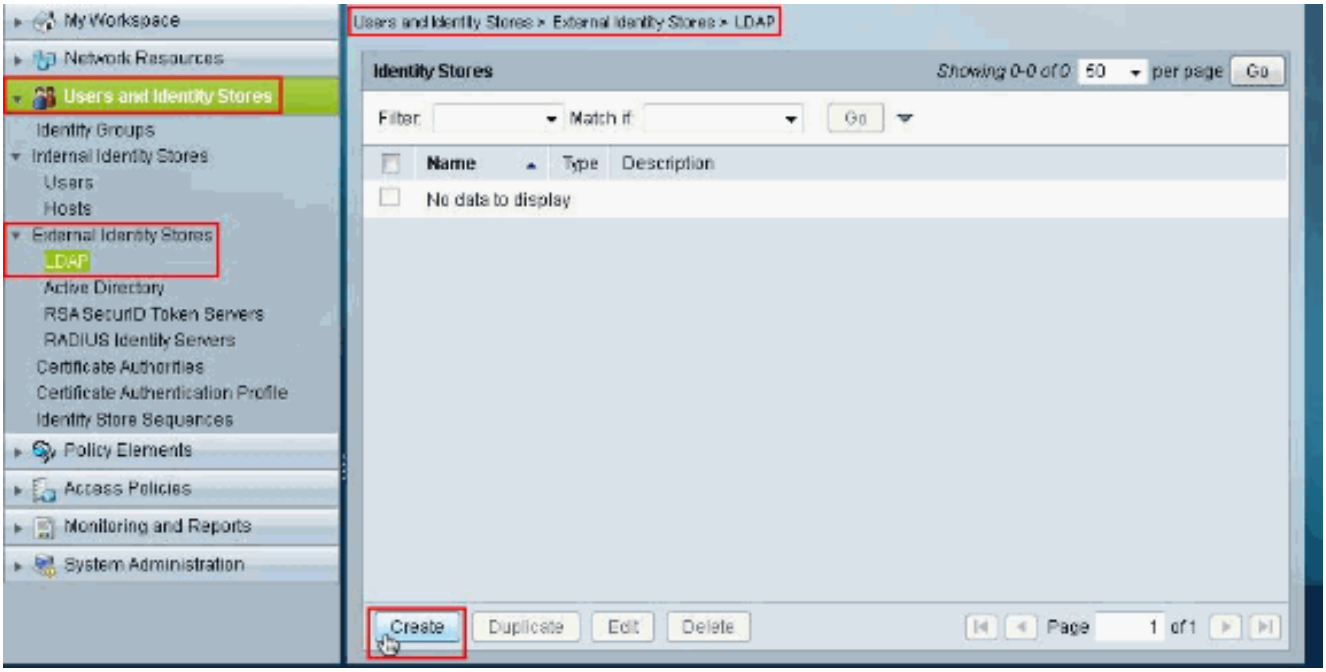
Esta imagen muestra que el certificado raíz ha estado instalado correctamente:



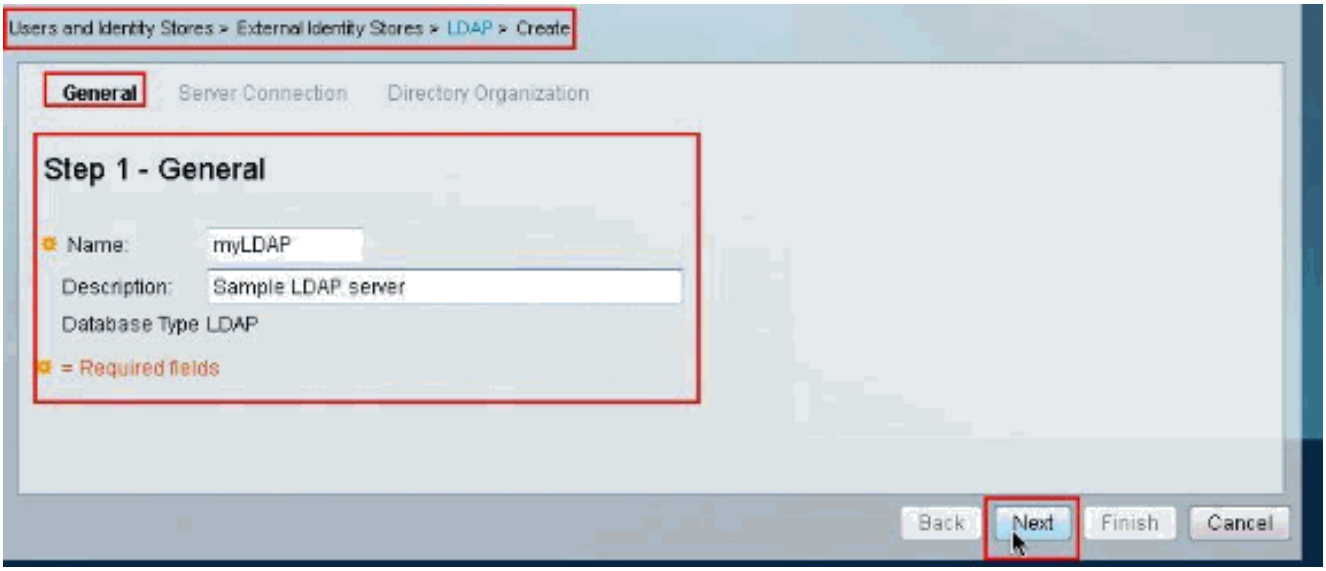
Configuración ACS 5.X para el LDAP seguro

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

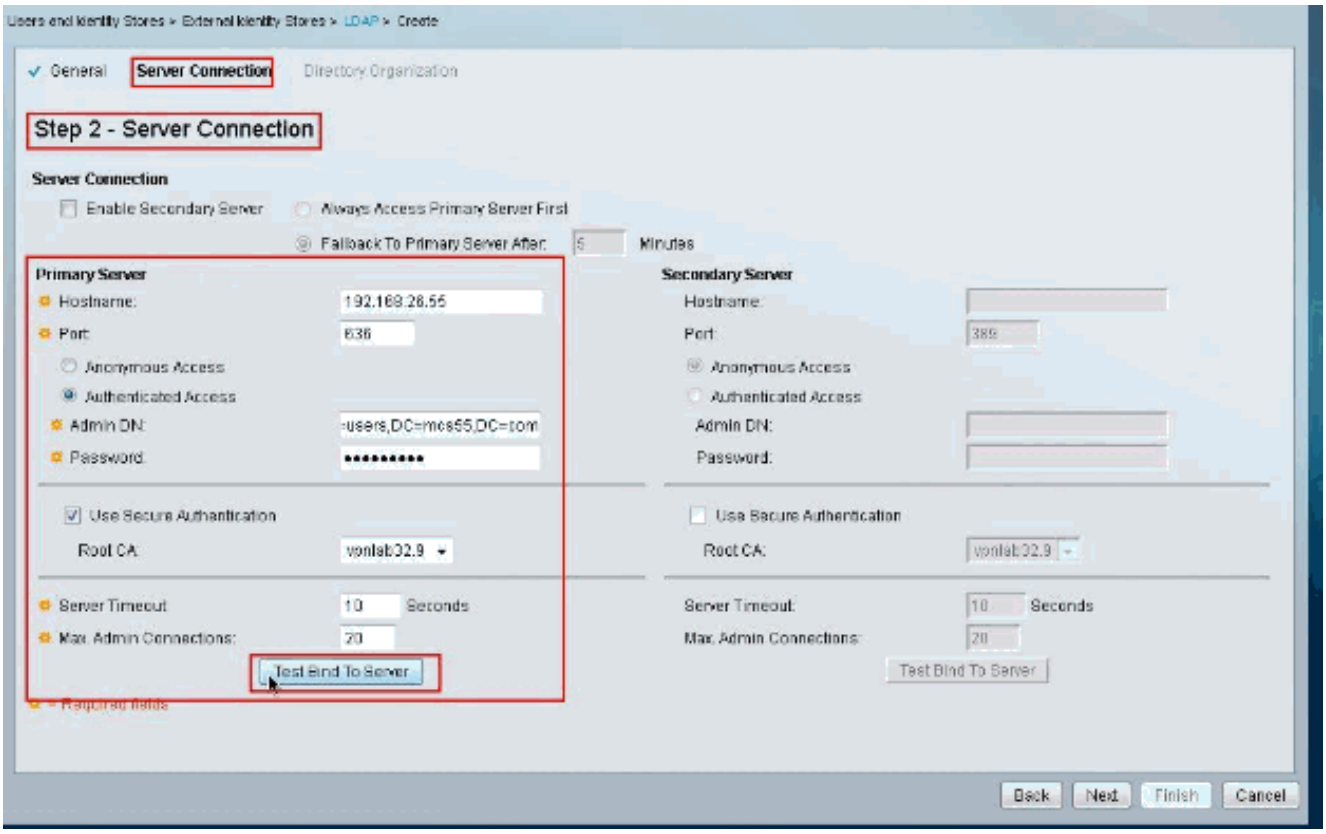
1. Elija a los **usuarios y la identidad salva > identidad externa salva > LDAP** y tecleo **crea** para crear una nueva conexión
LDAP.



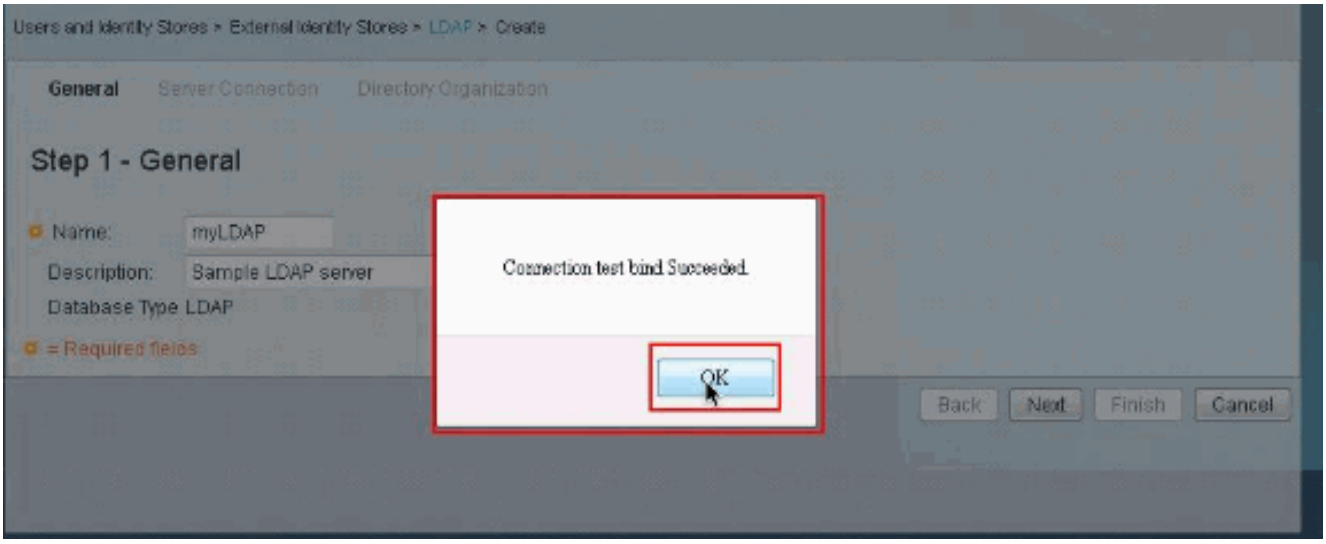
2. **De la ficha general** proporcione el **nombre** y el **Description(optional)** para el nuevo LDAP, después haga clic
después.



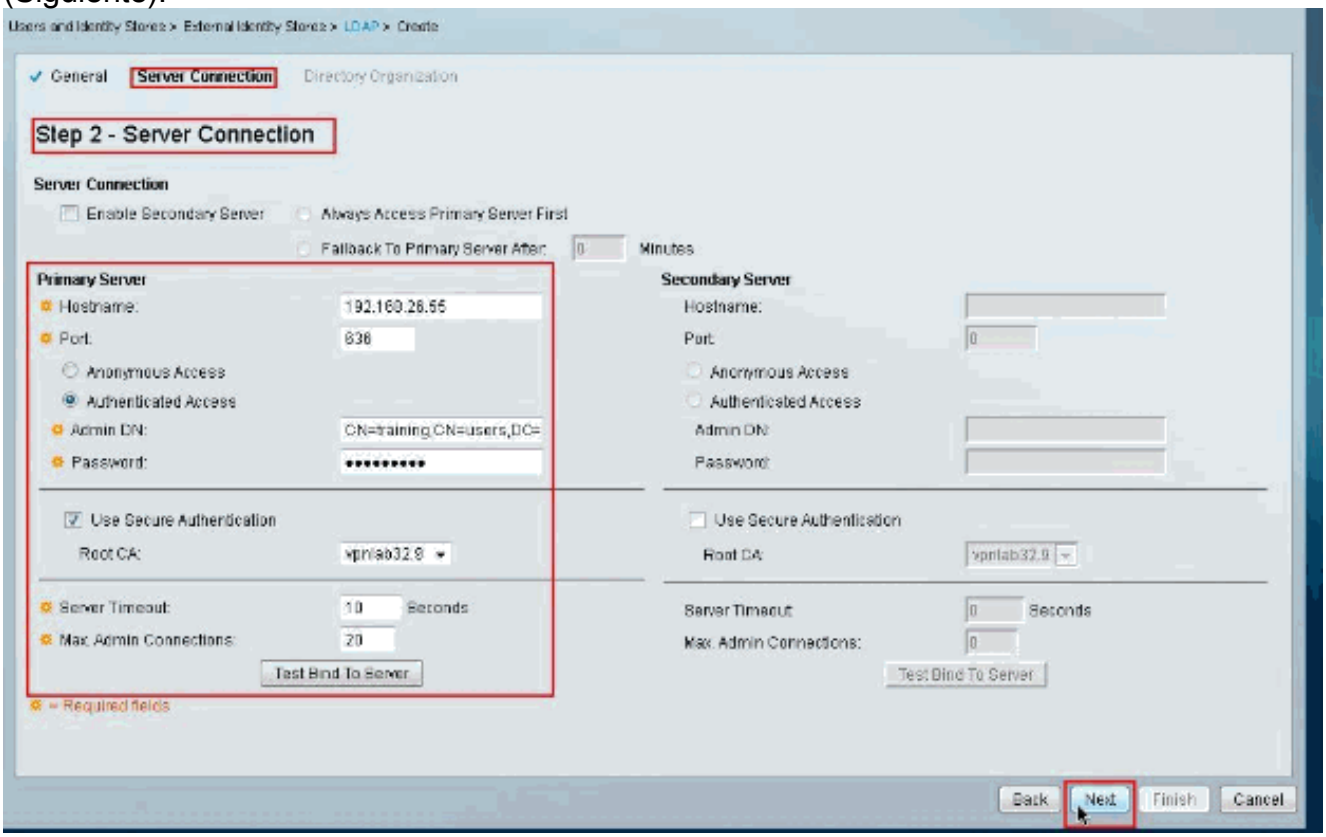
3. De la lengueta de la **conexión del servidor** bajo sección del **servidor primario**, proporcione el **nombre de host, el puerto, el Admin DN y la contraseña**. Asegúrese de que el checkbox al lado de la **autenticación segura del uso** esté marcado y elija instalado recientemente **certificado raíz CA**. Haga clic el **lazo de la prueba al servidor**.**Nota:** El número del puerto asignado IANA para el LDAP seguro es TCP 636. Sin embargo, confirme el número del puerto que su servidor LDAP está utilizando de su LDAP Admin.**Nota:** El Admin DN y contraseña se debe proporcionarle por su LDAP Admin. El Admin DN debe haber leído todos los permisos en todos los OU en el servidor LDAP.



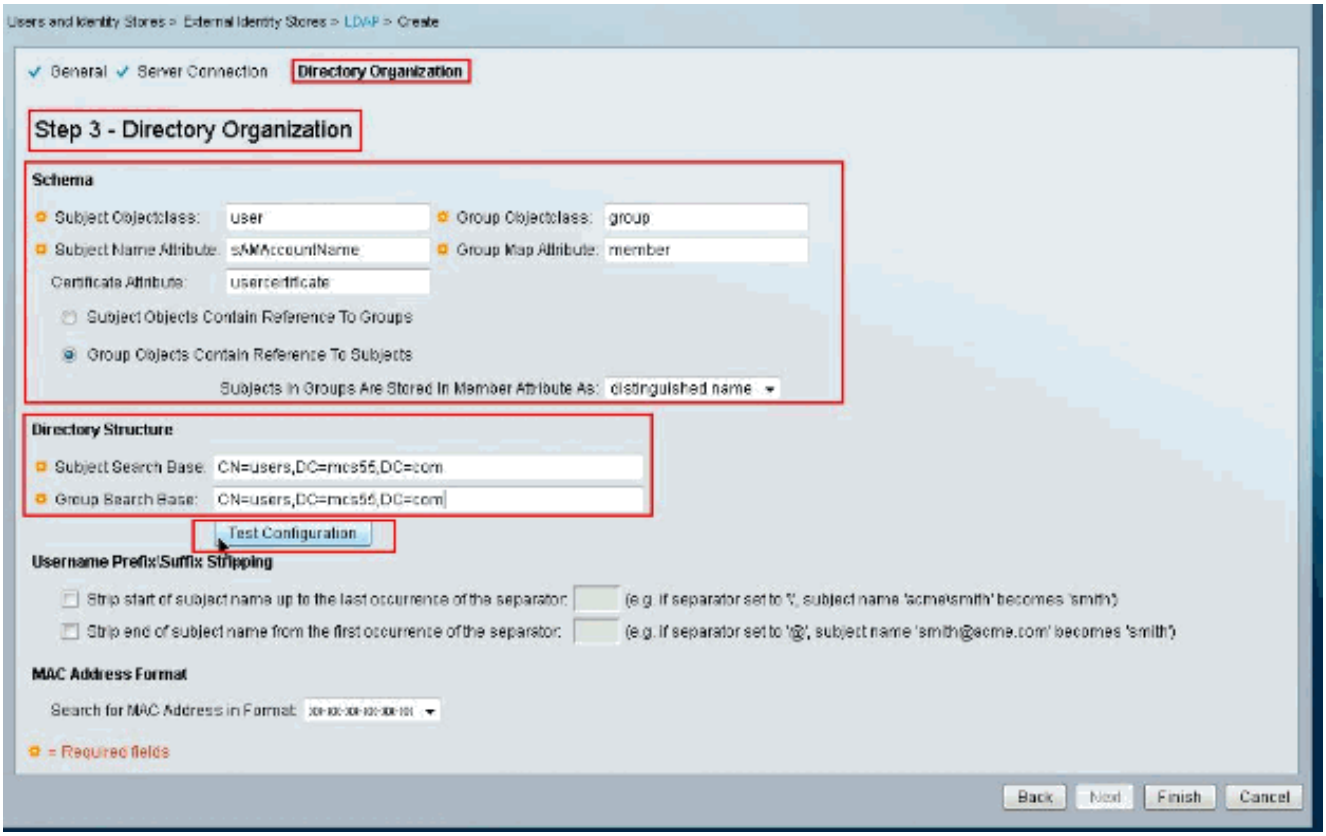
La imagen siguiente muestra que el **lazo de la prueba de la conexión al servidor** era acertado.**Nota:** Si el lazo de la prueba no es acertado entonces re-verifique el **nombre de host, número del puerto, Admin DN, contraseña** y **raíz CA de** su administrador LDAP.



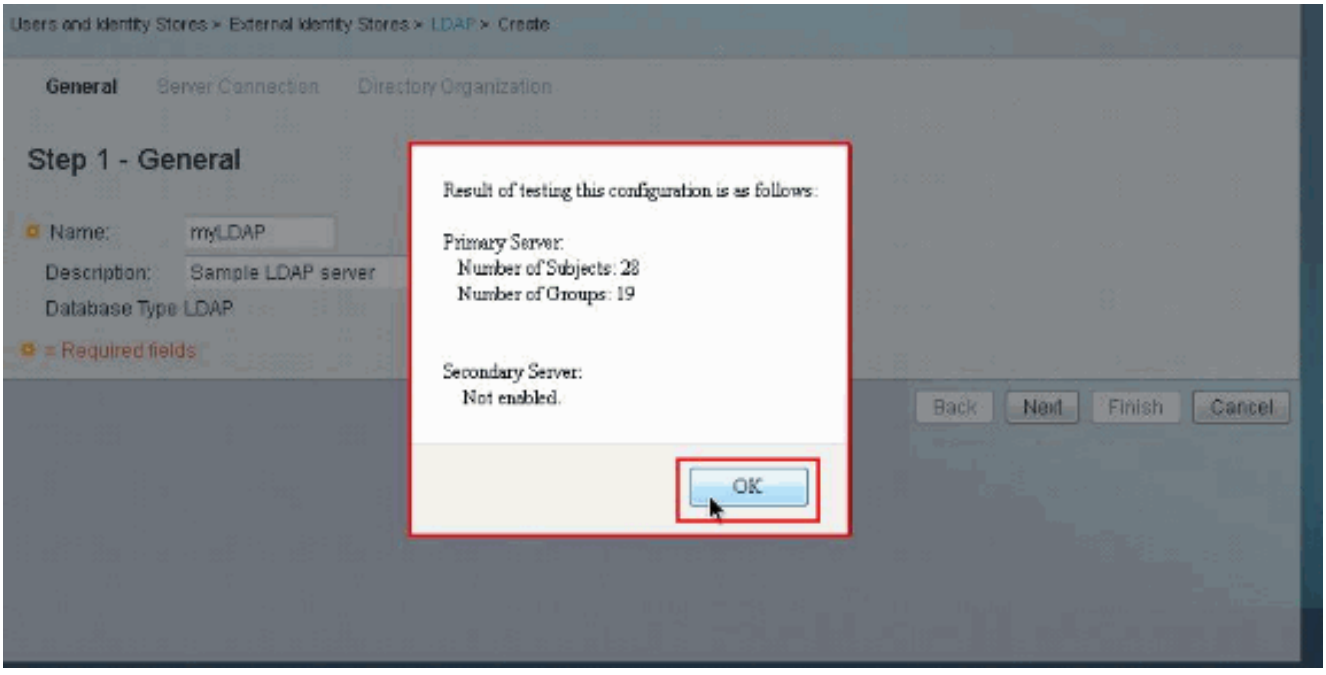
4. Haga clic en Next (Siguiente).



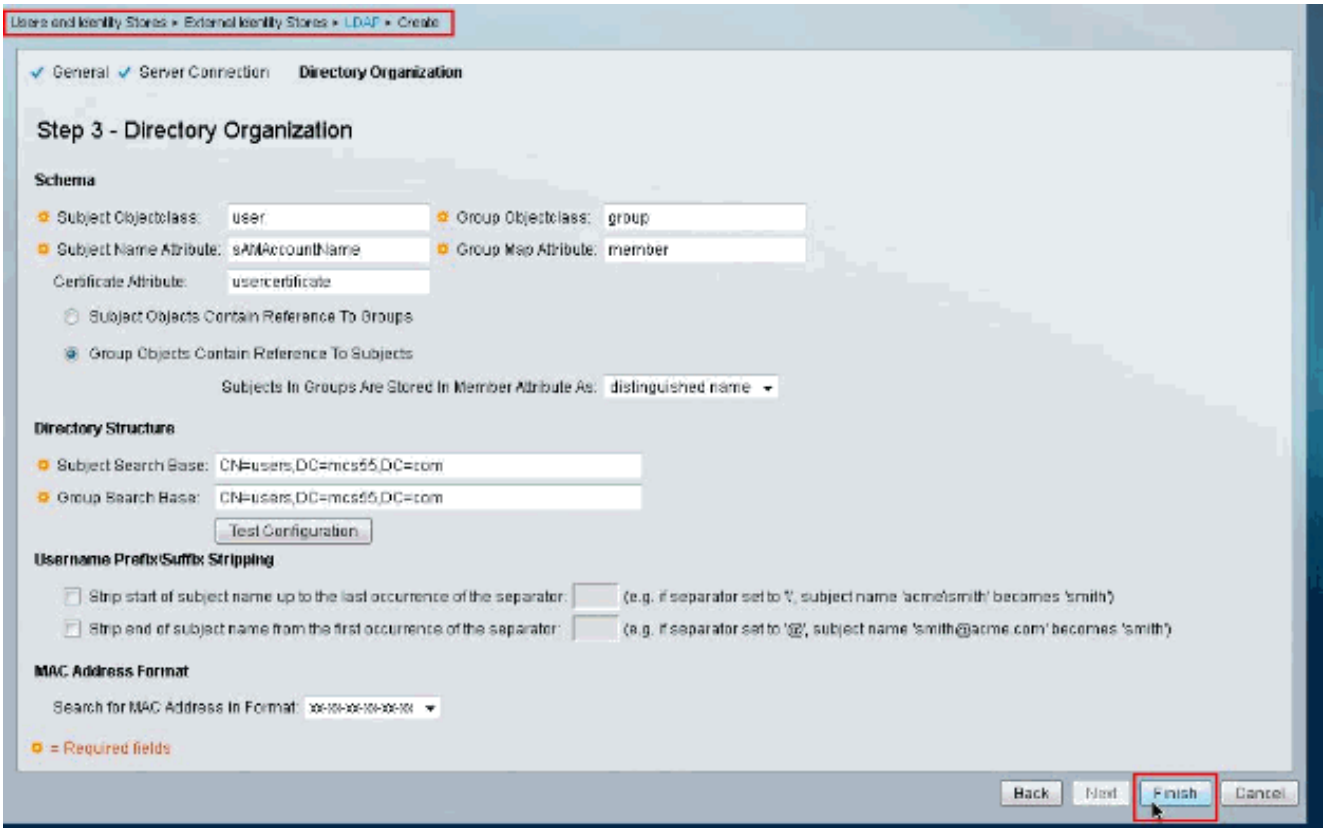
5. De la lengueta de la **organización del directorio** bajo sección del **esquema**, proporcione los detalles requeridos. Semejantemente, proporcione la Información requerida bajo sección de la **estructura de directorios** como está previsto por su LDAP Admin. Haga clic la **configuración de la prueba**.



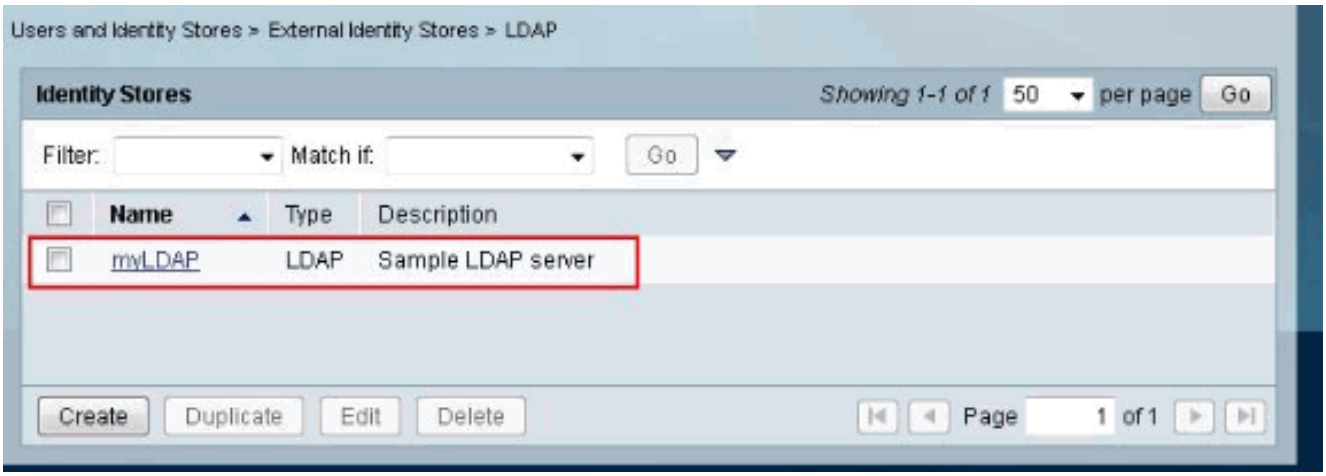
La imagen siguiente muestra que la **prueba de la configuración** es acertada.**Nota:** Si la prueba de la configuración no es acertada entonces re-verifique los parámetros proporcionados en el **esquema** y la **estructura de directorios de** su administrador LDAP.



6. Haga clic en Finish (Finalizar).



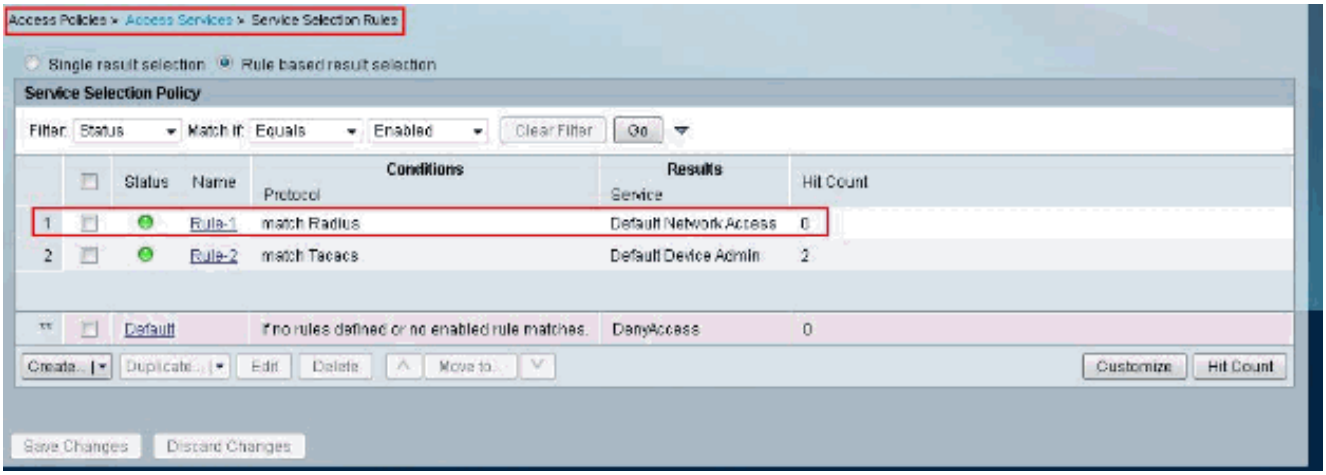
Crean al **servidor LDAP** con éxito.



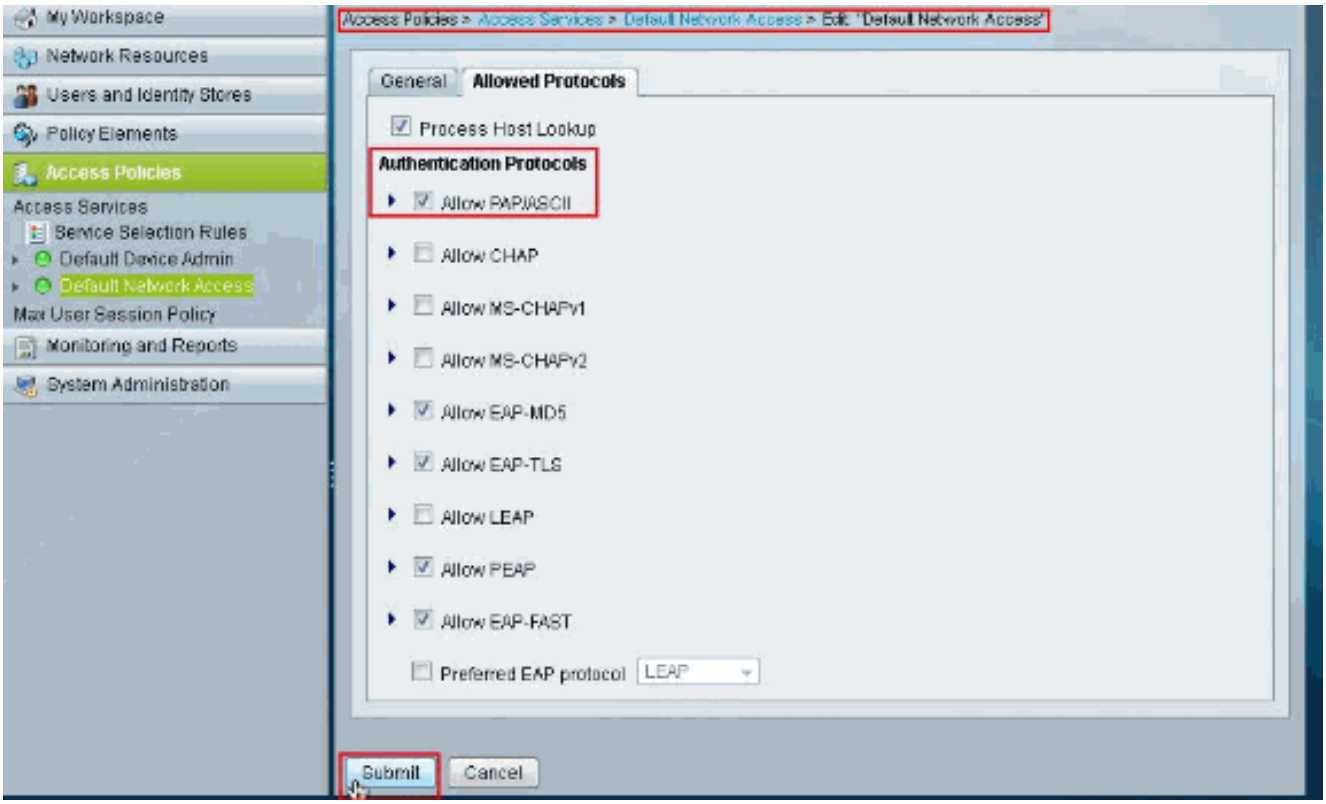
Configure el almacén de la identidad

Compiten estos pasos para configurar el almacén de la identidad:

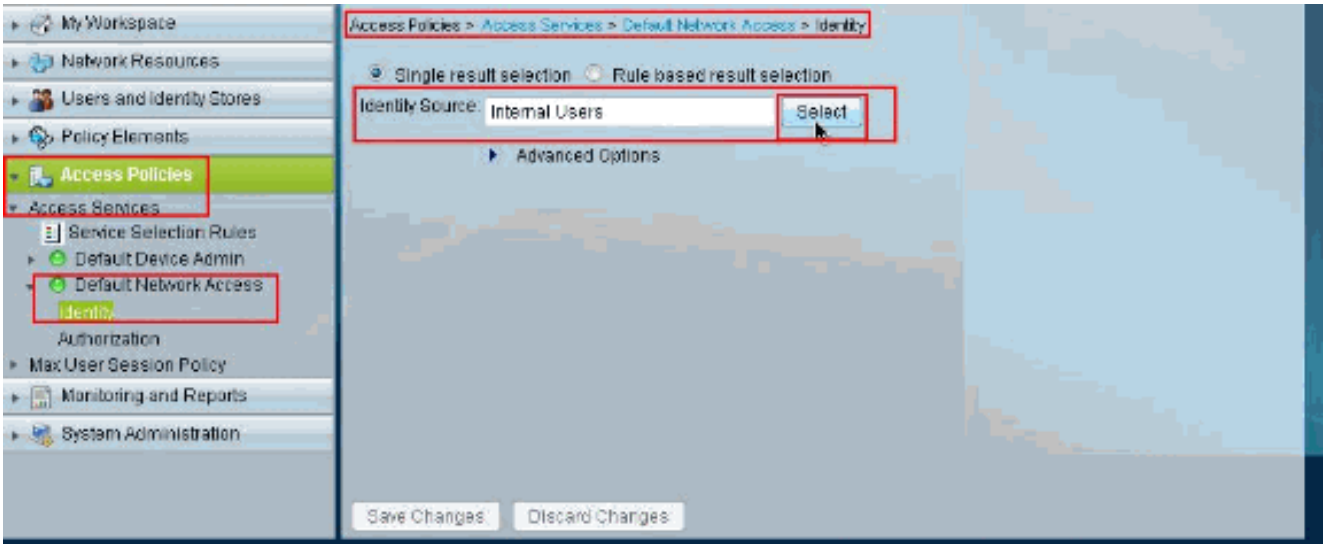
1. Elija las **políticas de acceso > el acceso mantiene > las reglas de selección del servicio** y verifica qué servicio va a utilizar asegura al servidor LDAP para la autenticación. En este ejemplo el servicio es **acceso de red predeterminada**.



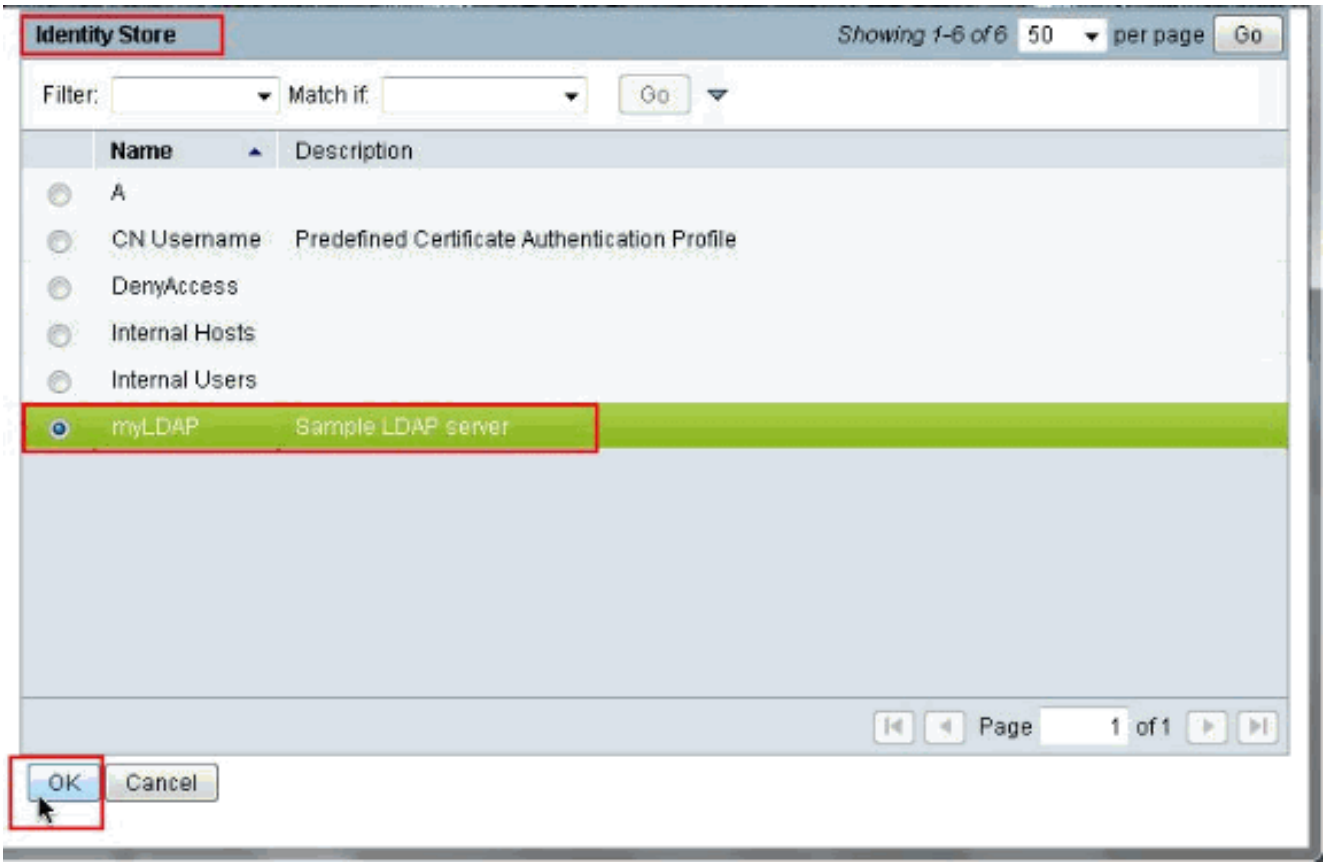
2. Después de que usted haya verificado el servicio en el paso 1, vaya al servicio determinado y haga clic los **protocolos permitidos**. Asegúrese que **permite PAP/ASCII** se selecciona, después hace clic **somete**.**Nota:** Usted puede tener otros Protocolos de autenticación seleccionados con para permitir
PAP/ASCII.



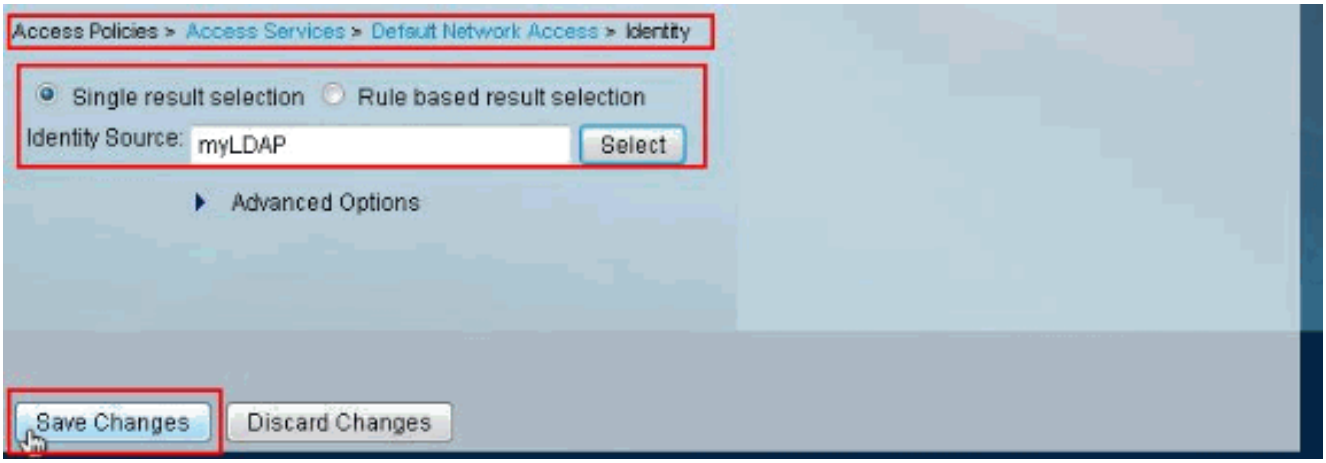
3. Haga clic el servicio identificado en el paso 1, después haga clic la **identidad**. Haga clic **selecto** al lado de la **fuente de la identidad**.



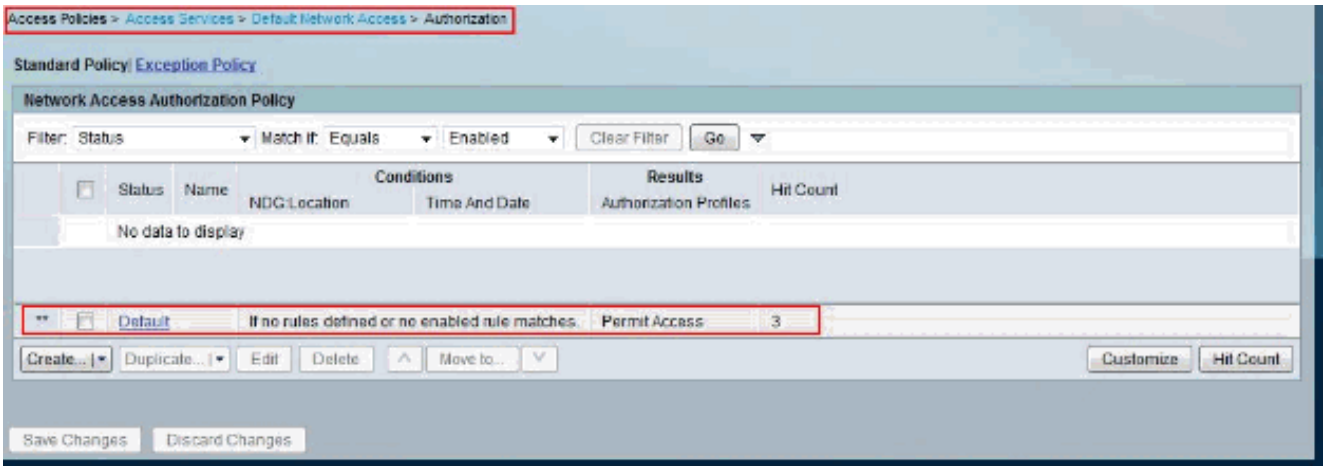
4. Seleccione el creado recientemente **aseguran al servidor LDAP** (**myLDAP** en este ejemplo), después hacen clic la **AUTORIZACIÓN**.



5. Haga clic los **cambios de la salvaguardia**.



6. Vaya a la sección de la **autorización del** servicio identificado en el **paso 1** y asegúrese de 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 restricta (inhabilitado, bloqueado hacia fuera, expirado, la contraseña expiró, y así sucesivamente)

Estos errores se registran como errores del recurso externo, que indica 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

Este error se registra como error del usuario desconocido: `Un usuario no existe en la base de datos.`

Este error se registra como error de la contraseña no válida, donde existe el usuario, pero la contraseña enviada es inválida: `Una contraseña no válida fue ingresada.`

Información Relacionada

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