ACS 5.X: Fixe o exemplo de configuração do servidor ldap

Índice

Introdução

O Lightweight Directory Access Protocol (LDAP) é um protocolo de rede para os serviços de diretório de pergunta e de alteração que são executado no TCP/IP e no UDP. O LDAP é um mecanismo leve para acessar um servidor de diretório baseado em x.500. O RFC 2251 define o LDAP.

O Access Control Server (ACS) 5.x integra com um base de dados externo LDAP, igualmente chamado uma loja da identidade, usando o protocolo ldap. Há dois métodos a conectar ao servidor ldap: texto simples (simples) e conexão SSL (cifrado). O ACS 5.x pode ser configurado para conectar ao servidor ldap usando ambos os métodos. Neste documento o ACS 5.x é configurado para conectar a um servidor ldap usando a conexão criptografada.

Pré-requisitos

Requisitos

Este documento supõe que o ACS 5.x tem uma conexão IP ao servidor ldap e a porta TCP 636 está aberta.

O servidor ldap do diretório ativo de Microsoft® precisa de ser configurado para aceitar fixa conexões ldap na porta TCP 636. Este documento supõe que você tem o certificado de raiz do Certification Authority (CA) que emitiu o certificado de servidor ao servidor ldap de Microsoft. Para obter mais informações sobre de como configurar o servidor ldap, refira como permitir o LDAP sobre o SSL com uma autoridade de certificação da terceira.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure ACS 5.x
- Servidor ldap do microsoft ative directory

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Serviço de diretório

O serviço de diretório é um aplicativo de software, ou um grupo de pedidos, para a informação de armazenagem e de organização sobre os usuários e os recursos de rede de uma rede de computador. Você pode usar o serviço de diretório para controlar o acesso de usuário a estes recursos.

O serviço de diretório LDAP é baseado em um client-server model. Um cliente começa uma sessão LDAP conectando a um servidor ldap, e envia pedidos da operação ao server. O server envia então suas respostas. Uns ou vários servidores ldap contêm dados da árvore de diretório LDAP ou do base de dados da parte posterior LDAP.

O serviço de diretório controla o diretório, que é o base de dados que guarda a informação. Os serviços de diretório usam um modelo distribuído armazenando a informação, e essa informação replicated geralmente entre servidores de diretório.

Um diretório LDAP é organizado em uma hierarquia da árvore simples e pode ser distribuído entre muitos server. Cada server pode ter uma versão replicated do diretório total que é sincronizado periodicamente.

Uma entrada na árvore contém um grupo de atributos, onde cada atributo tem um nome (um tipo do atributo ou uma descrição do atributo) e uns ou vários valores. Os atributos são definidos em um esquema.

Cada entrada tem um identificador exclusivo: seu nome destacado (DN). Este nome contém o nome destacado relativo (RDN) construído dos atributos na entrada, seguida pelo DN da entrada do pai. Você pode pensar do DN como um nome de arquivo completo, e do RDN como um nome de arquivo relativo em um dobrador.

Autenticação usando o LDAP

O ACS 5.x pode autenticar um principal contra uma loja da identidade LDAP executando uma operação do ligamento no servidor de diretório para encontrar e autenticar o principal. Se a

autenticação sucede, o ACS pode recuperar os grupos e os atributos que pertencem ao principal. Os atributos a recuperar podem ser configurados na interface da WEB ACS (páginas LDAP). Estes grupos e atributos podem ser usados pelo ACS para autorizar o principal.

A fim autenticar um usuário ou perguntar a loja da identidade LDAP, o ACS conecta ao servidor ldap e mantém um pool da conexão.

Gerenciamento da conexão ldap

O ACS 5.x apoia conexões ldap simultâneas múltiplas. As conexões são por encomenda aberto na altura da primeira autenticação LDAP. O número máximo de conexão é configurado para cada servidor ldap. Abrir conexões encurta adiantado o tempo da autenticação.

Você pode ajustar o número máximo de conexão para usar-se para conexões obrigatórias simultâneas. O número de conexões abertas pode ser diferente para cada servidor ldap (preliminar ou secundário) e é determinado de acordo com o número máximo de conexões da administração configuradas para cada server.

O ACS retém uma lista de conexões ldap abertas (que incluem a informação do ligamento) para cada servidor ldap que é configurado no ACS. Durante o processo de autenticação, o gerenciador de conexão tenta encontrar uma conexão aberta do pool.

Se uma conexão aberta não existe, um novo está aberto. Se o servidor ldap fechou a conexão, o gerenciador de conexão relata um erro durante a primeira chamada para procurar o diretório, e tenta-o renovar a conexão.

Depois que o processo de autenticação está completo, o gerenciador de conexão libera a conexão ao gerenciador de conexão. Para mais informação, refira o Guia do Usuário ACS 5.X.

Configurar

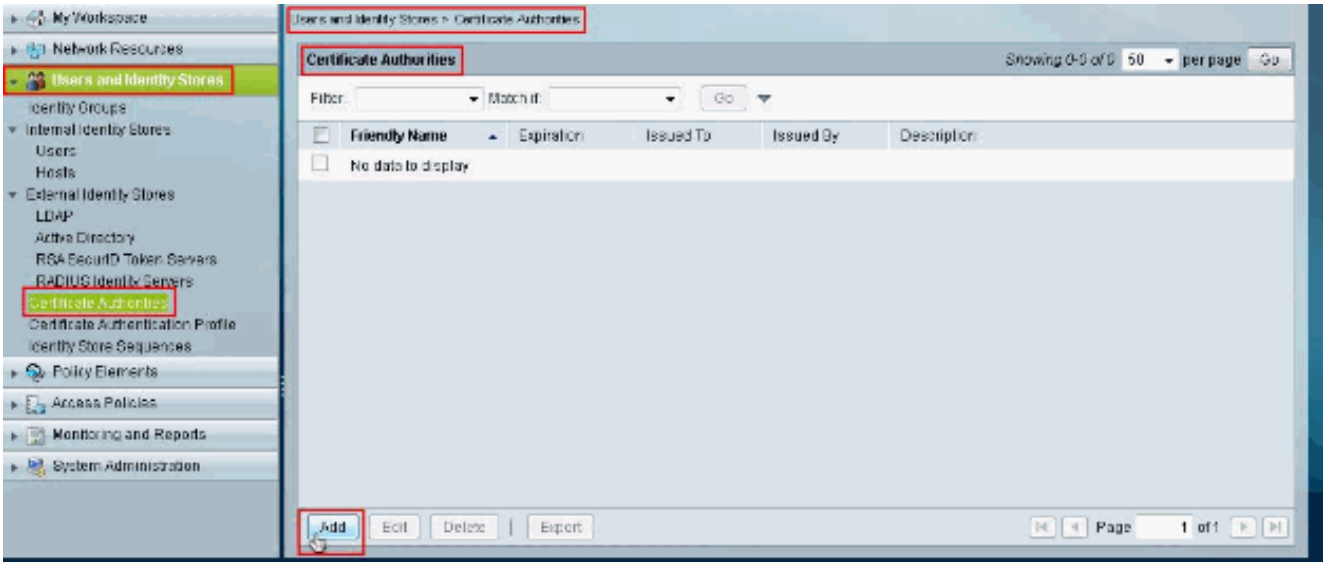
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Instale o certificado CA raiz em ACS 5.x

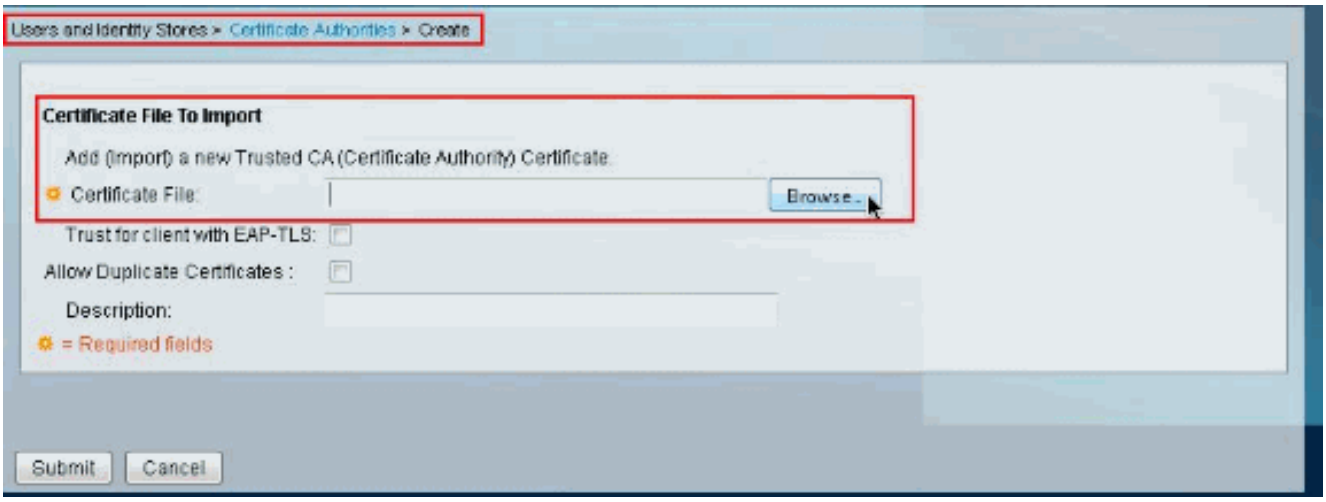
Termine estas etapas a fim instalar um certificado CA raiz no Cisco Secure ACS 5.x:

Nota: Assegure-se de que o servidor ldap PRE-esteja configurado para aceitar conexões criptografada na porta TCP 636. Para obter mais informações sobre de como configurar o servidor ldap de Microsoft, refira como permitir o LDAP sobre o SSL com uma autoridade de certificação da terceira.

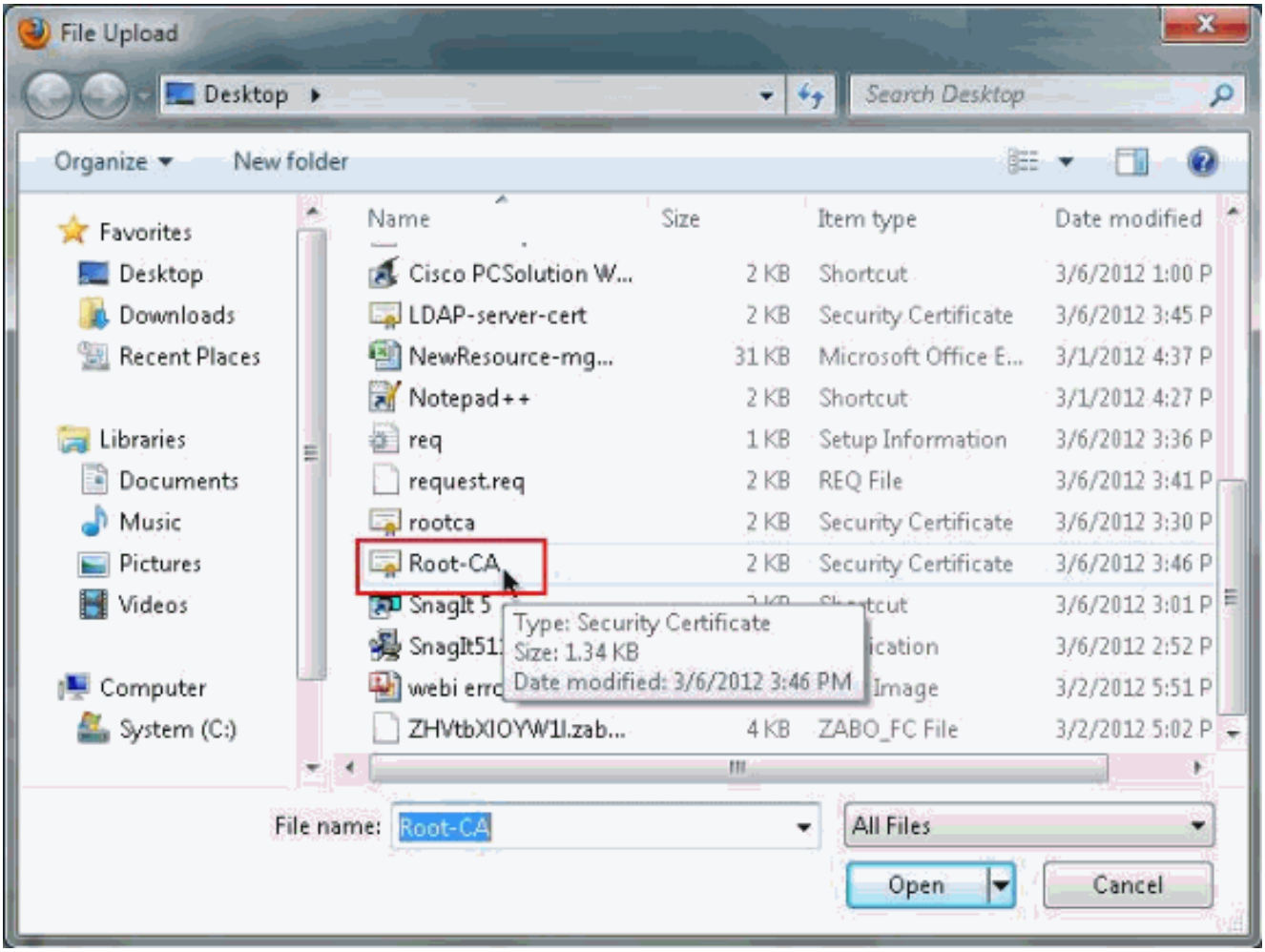
1. Escolha **usuários e a identidade armazena > autoridades de certificação**, a seguir clica **adiciona** a fim adicionar o certificado de raiz de CA que emitiu o certificado de servidor ao servidor ldap de
Microsoft.



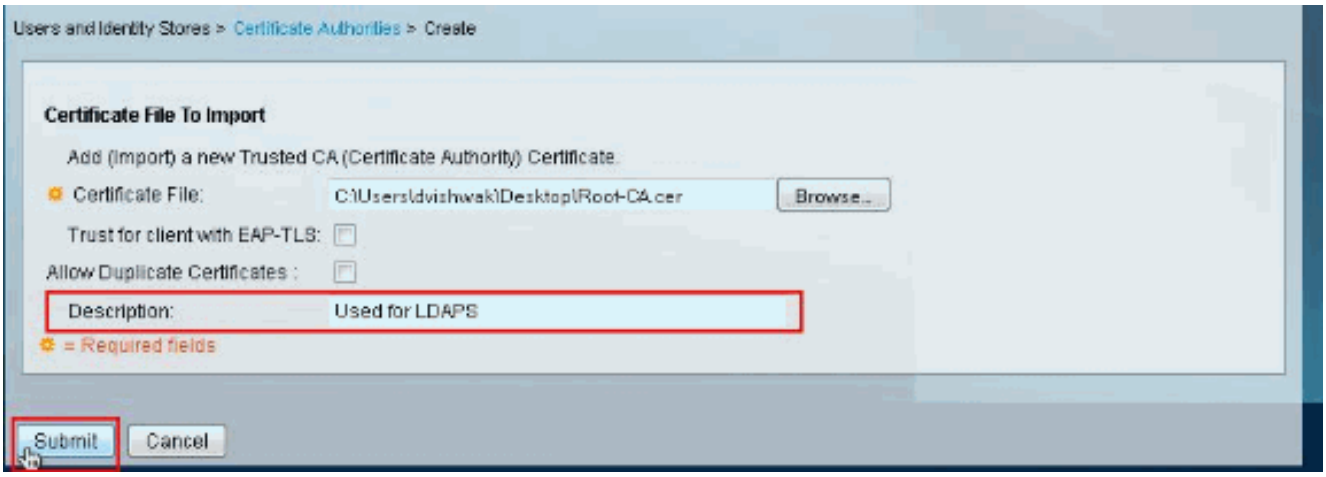
2. **Do arquivo certificado para importar a** seção, o clique **consulta** ao lado do **arquivo certificado** a fim procurar pelo arquivo
certificado.



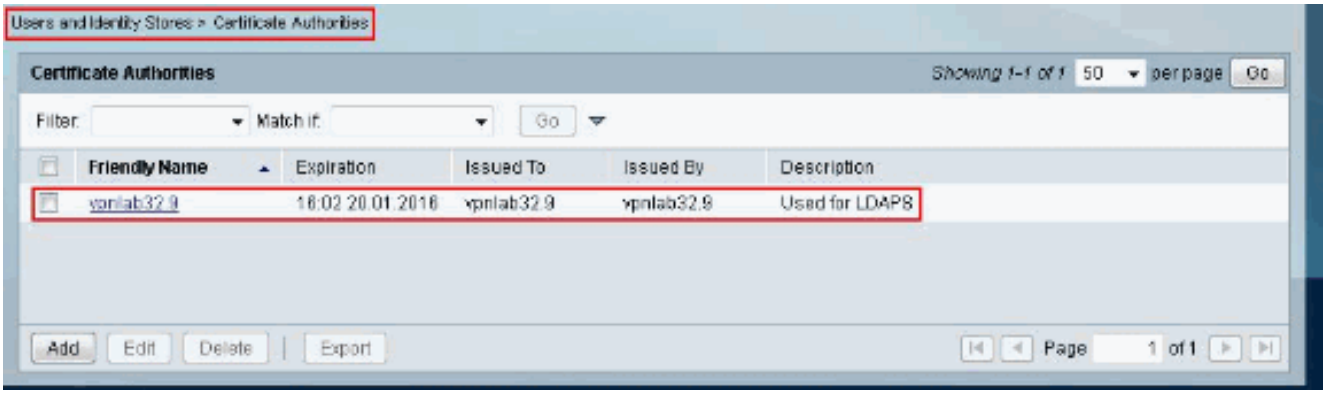
3. Escolha o **arquivo certificado** exigido (o certificado de raiz de CA que emitiu o certificado de servidor ao servidor ldap de Microsoft) e clique
aberto.



4. Forneça uma **descrição no** espaço fornecido ao lado da descrição e o clique **submete-se**.



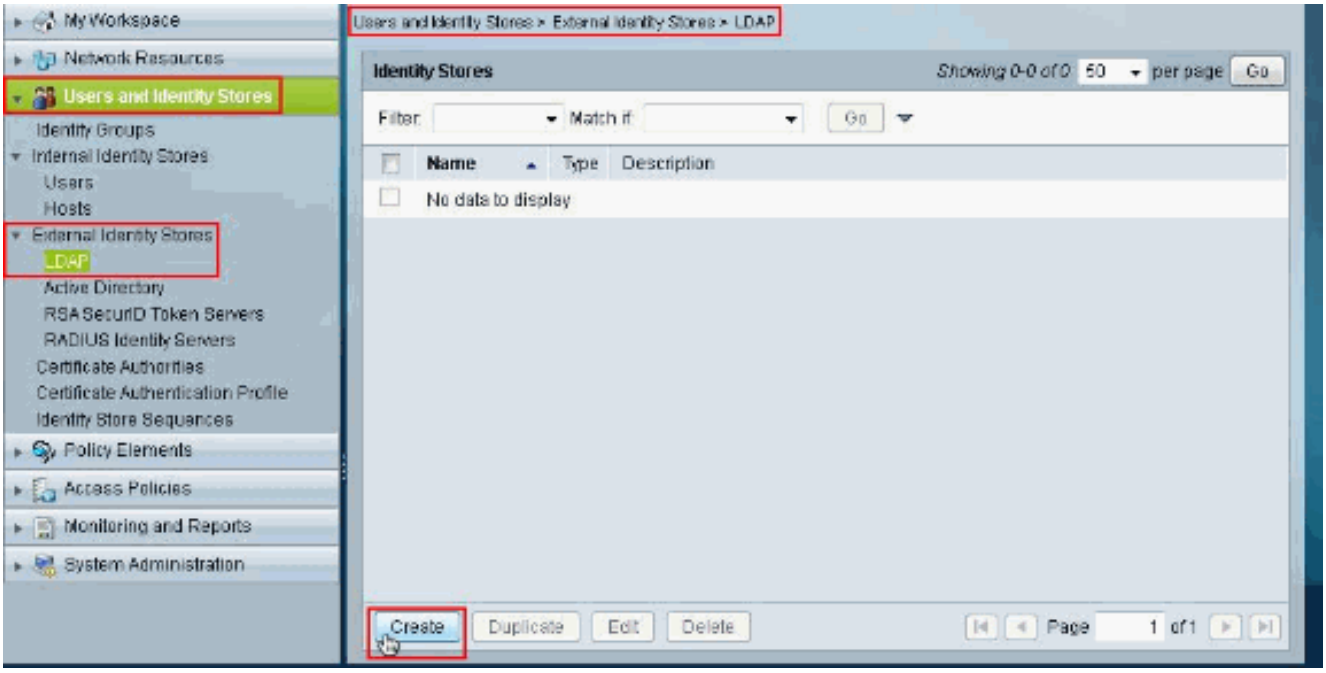
Esta imagem mostra que o certificado de raiz esteve instalado corretamente:



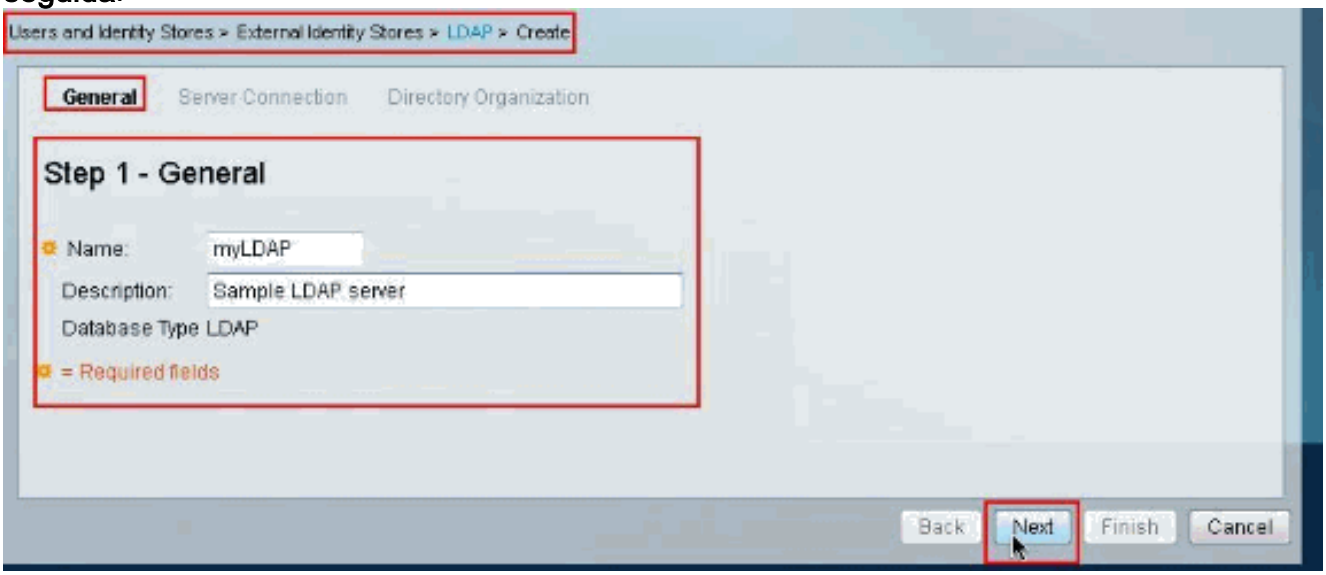
Configurar ACS 5.X para o LDAP seguro

Termine estas etapas a fim configurar ACS 5.x para o LDAP seguro:

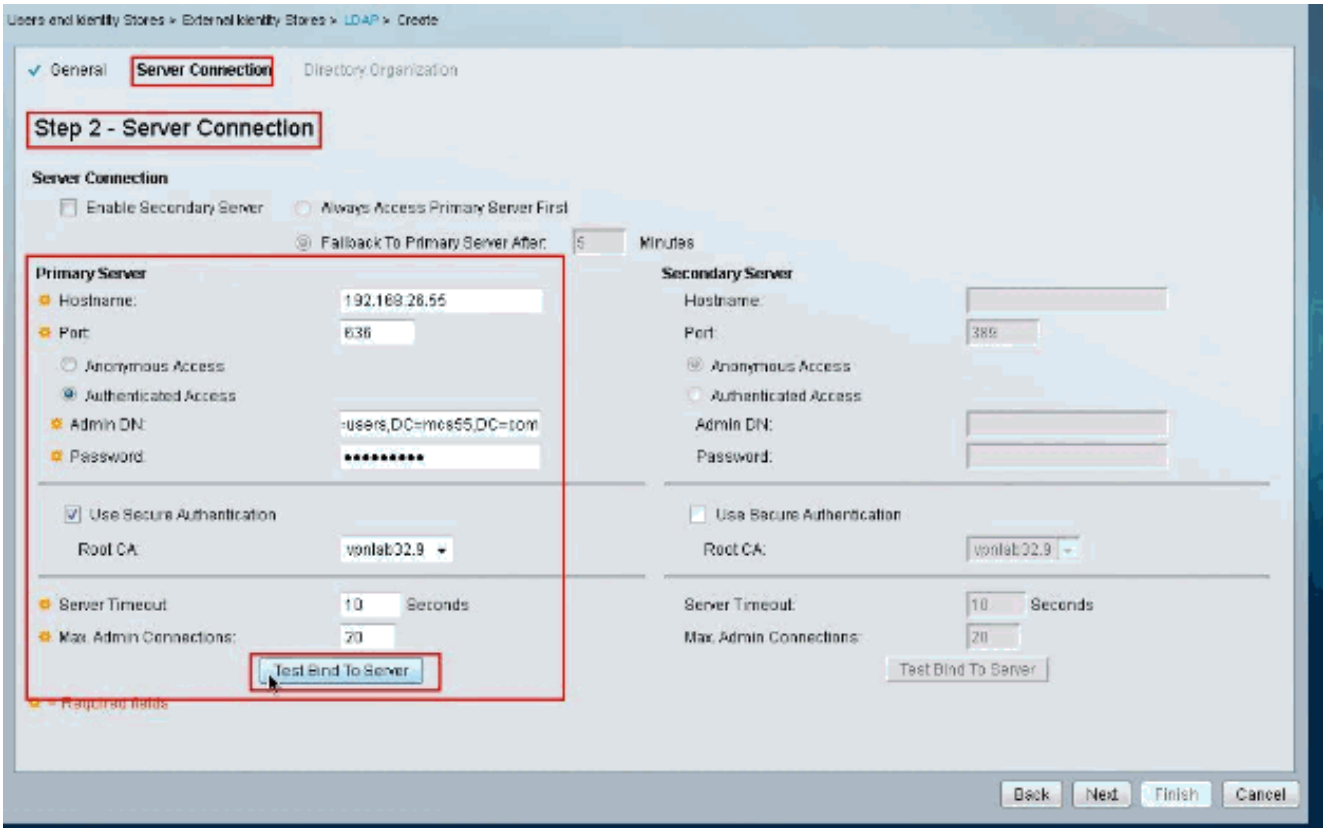
1. Escolha **usuários e a identidade armazena > identidade externo armazena > LDAP** e clique **cria** para criar uma conexão ldap nova.



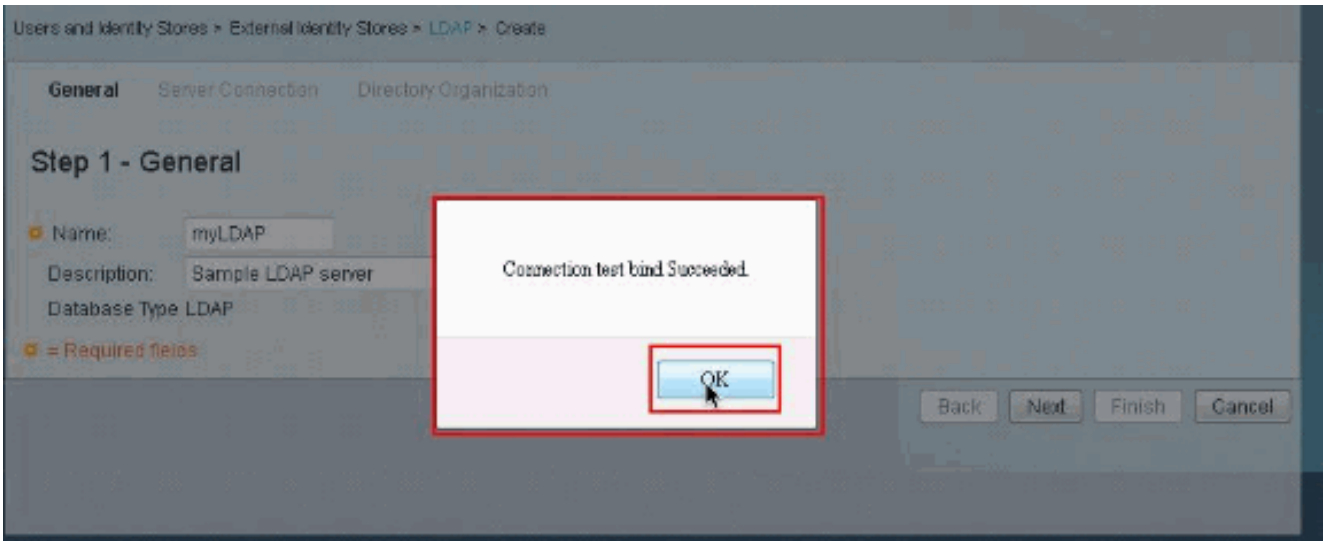
2. **Do tab geral** forneça o **nome** e o **Description(optional)** para o LDAP novo, a seguir clique-os **em seguida**.



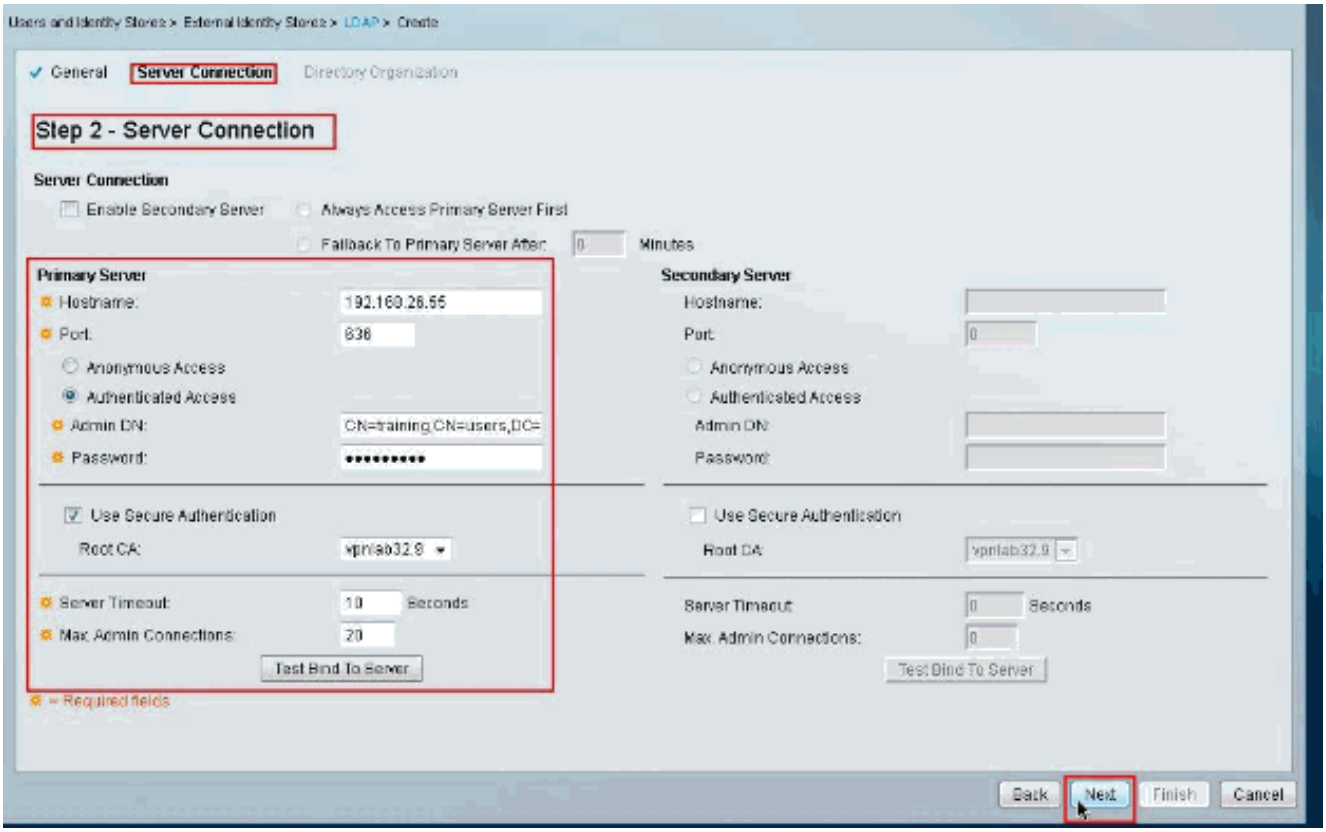
3. Da aba da **conexão de servidor** sob a seção do **servidor primário**, forneça o **hostname, a porta, o Admin DN e a senha**. Assegure-se de que a caixa de seleção ao lado da **autenticação segura do uso** esteja verificada e escolha-se o **certificado CA raiz** recentemente instalado. Clique o **ligamento do teste ao server**.**Nota:** O número de porta atribuído IANA para o LDAP seguro é TCP 636. Contudo, confirme o número de porta que seu servidor ldap está usando de seu LDAP Admin.**Nota:** O Admin DN e senha deve ser-lhe fornecido por seu LDAP Admin. O Admin DN deve ter lido todas as permissões em todos os OU no servidor ldap.



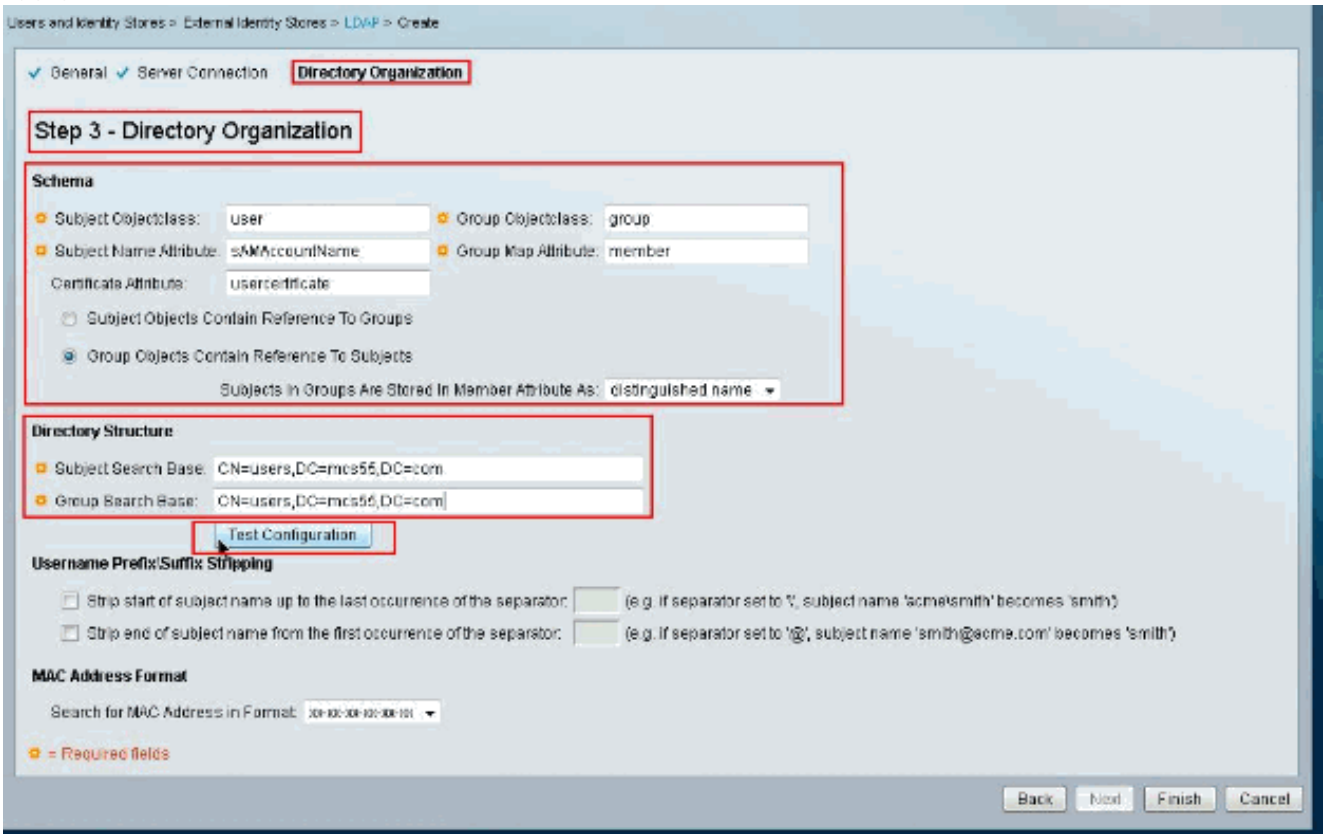
A imagem seguinte mostra que o **ligamento do teste da conexão ao server** era bem sucedido.**Nota:** Se o ligamento do teste não é bem sucedido então re-verifique o **hostname, o número de porta, o Admin DN, a senha** e a **CA raiz de** seu administrador LDAP.



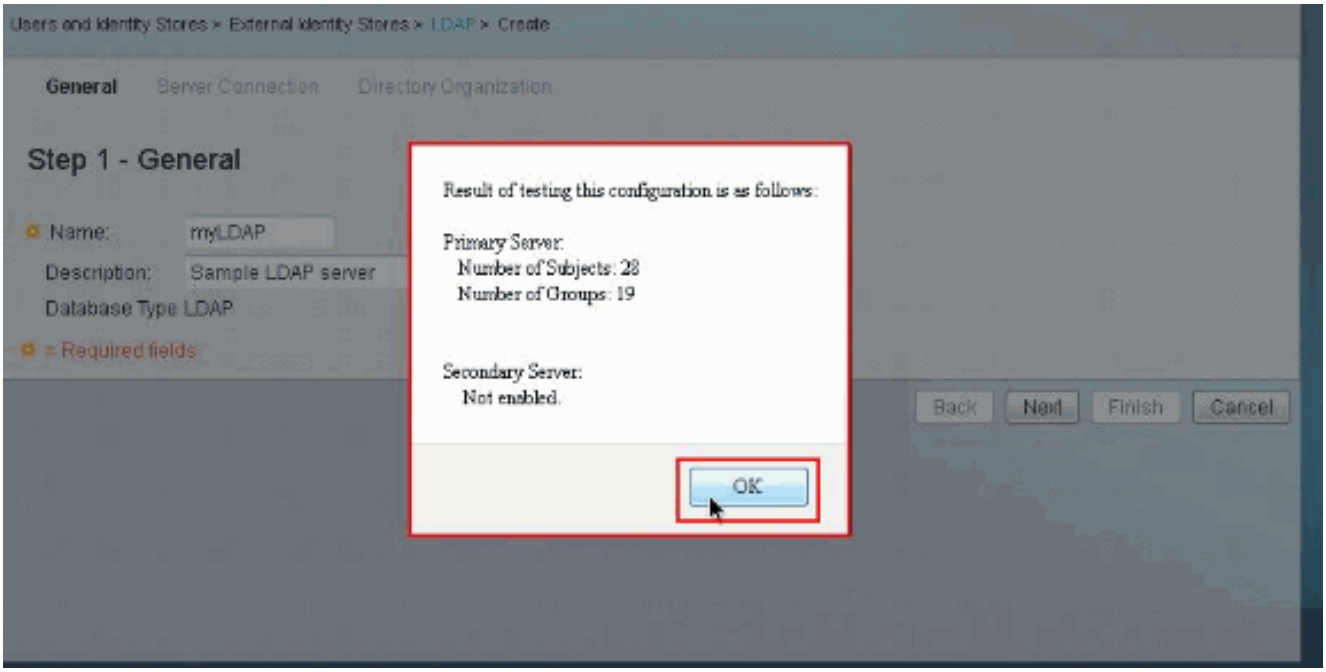
4. Clique em Next.



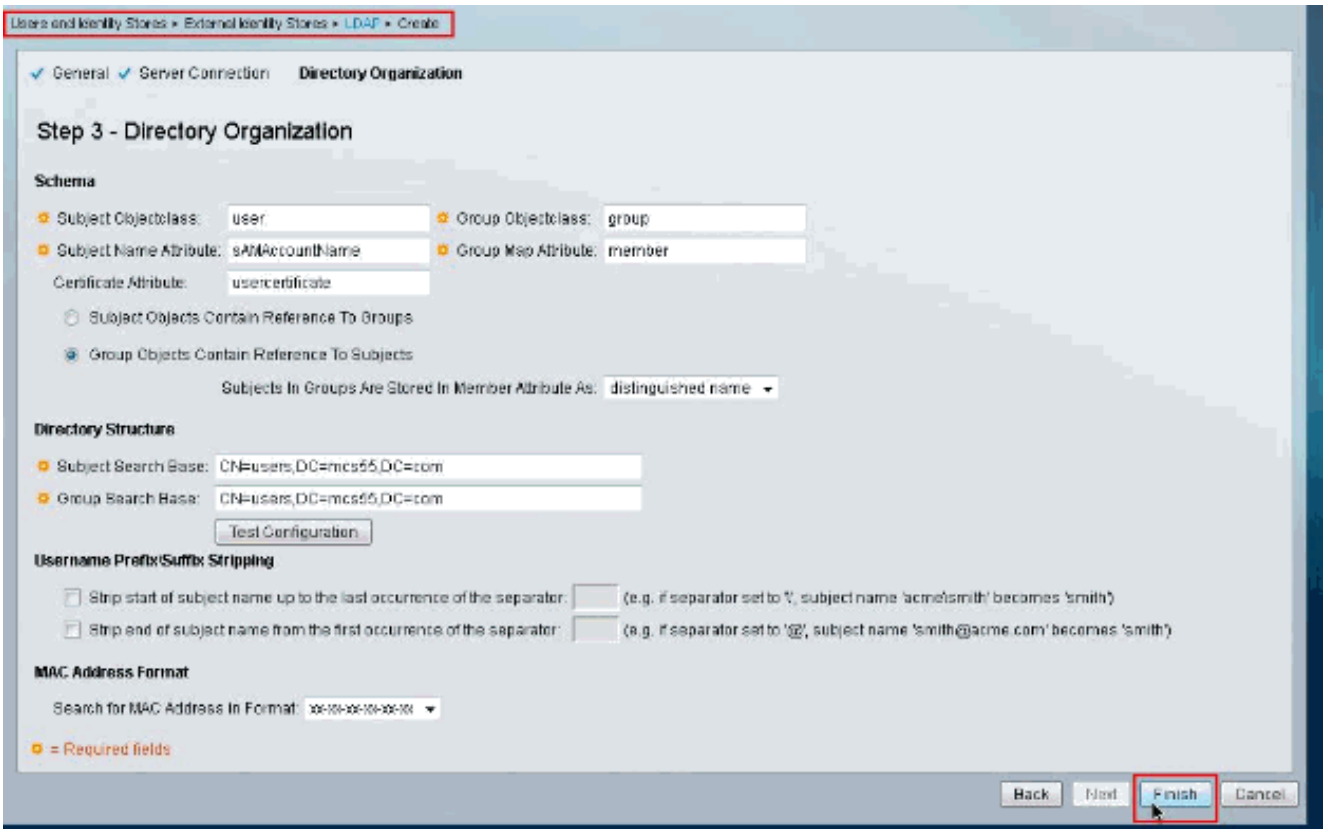
5. Da aba da **organização do diretório** sob a seção do **esquema**, forneça os detalhes exigidos. Similarmente, forneça a informação requerida sob a seção da **estrutura do diretório** da maneira prevista por seu LDAP Admin. Clique a **configuração do teste**.



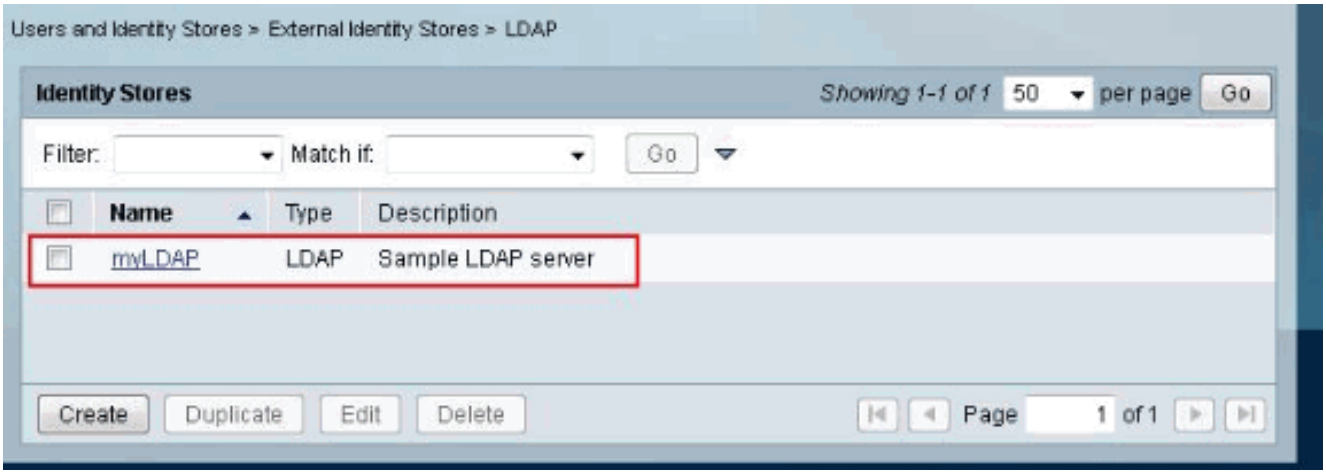
A imagem seguinte mostra que o **teste da configuração** é bem sucedido.**Nota:** Se o teste da configuração não é bem sucedido então re-verifique os parâmetros fornecidos no **esquema** e na **estrutura do diretório de** seu administrador LDAP.



6. Clique em Finish.



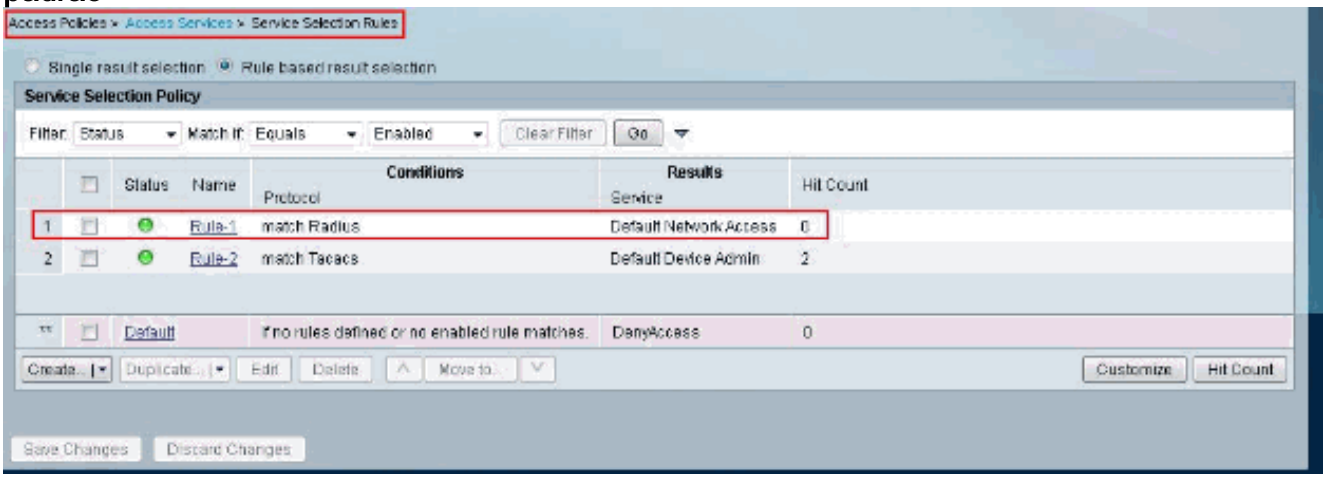
O servidor ldap é criado com sucesso.



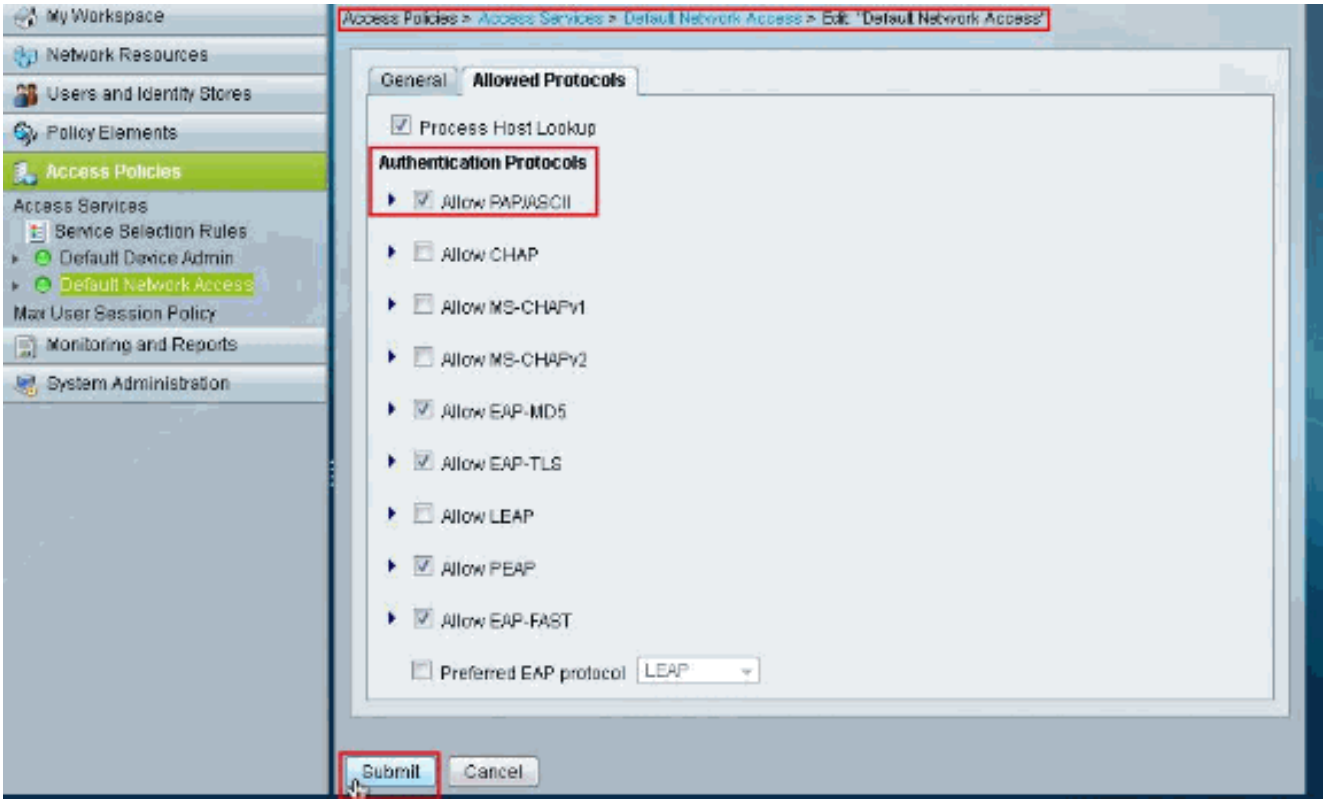
Configurar a loja da identidade

Competem estas etapas a fim configurar a loja da identidade:

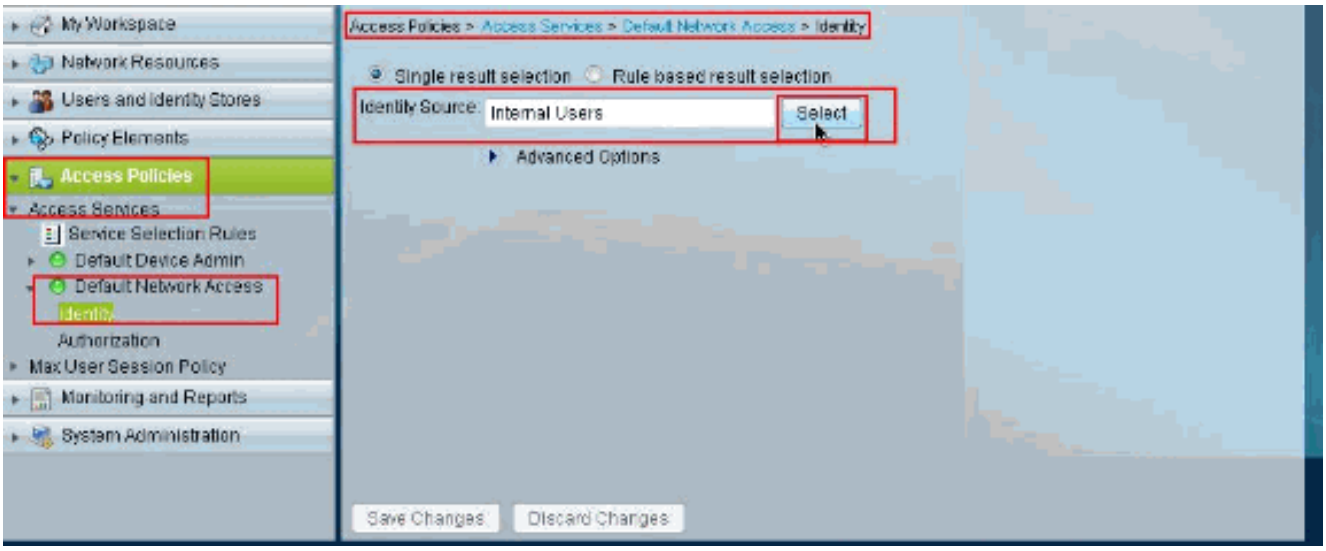
1. Escolha **políticas de acesso > acesso presta serviços de manutenção > regras de seleção do serviço** e verificam que que serviço está indo se usar fixe o servidor ldap para a autenticação. Neste exemplo o serviço é **acesso de rede padrão**.



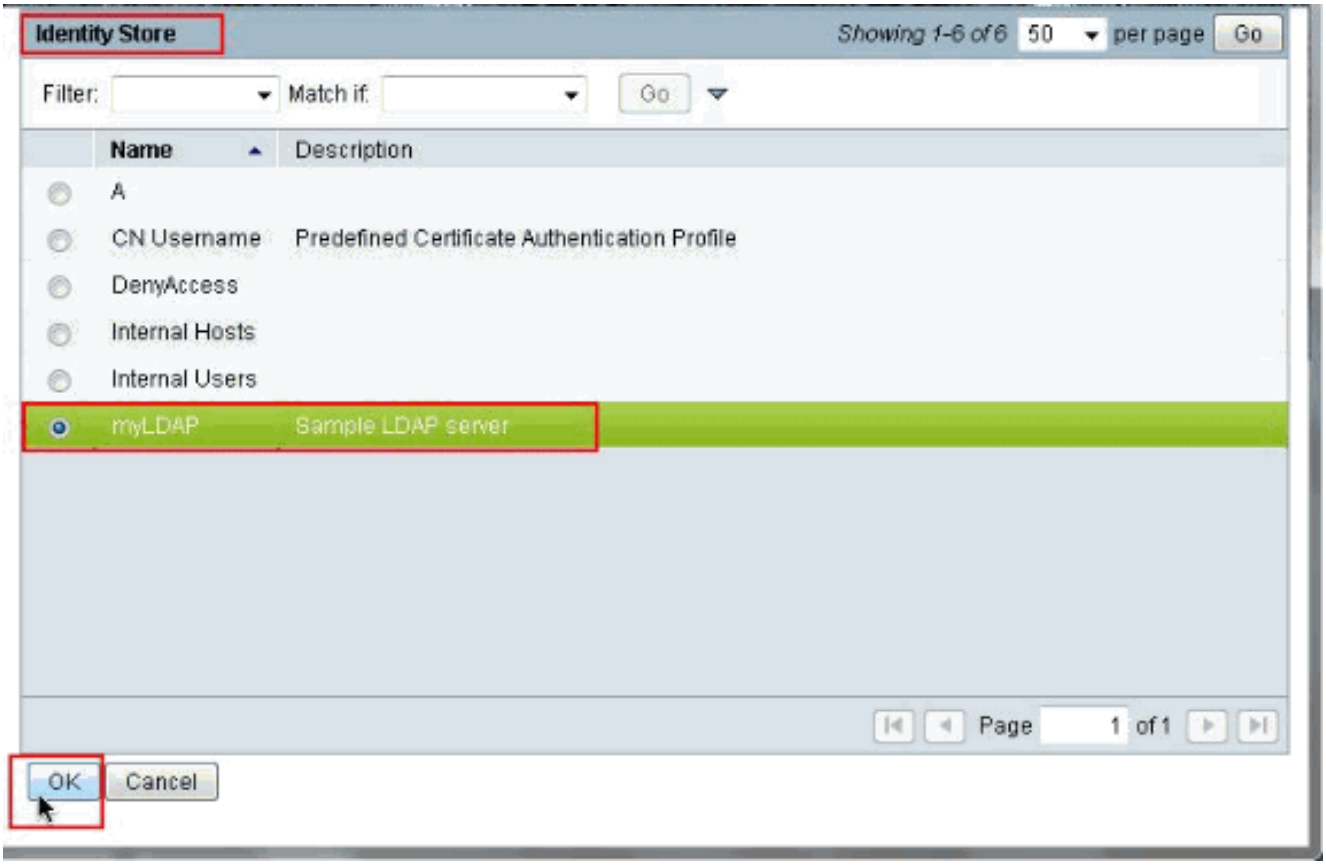
2. Depois que você verificou o serviço em etapa 1, vá ao serviço particular e clique **protocolos permitidos**. Assegure-se de que que **reserva PAP/ASCII** é selecionado, a seguir clica **submete-se**.**Nota:** Você pode ter outros Protocolos de autenticação selecionados com para permitir
PAP/ASCII.



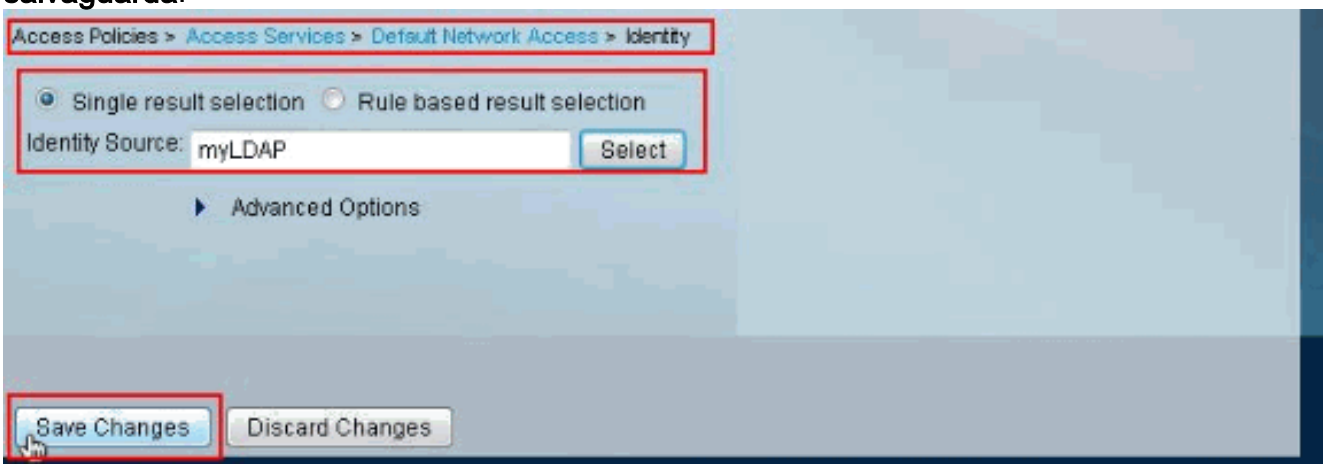
3. Clique o serviço identificado em etapa 1, a seguir clique a **identidade**. Clique **seleto** ao lado da **fonte da identidade**.



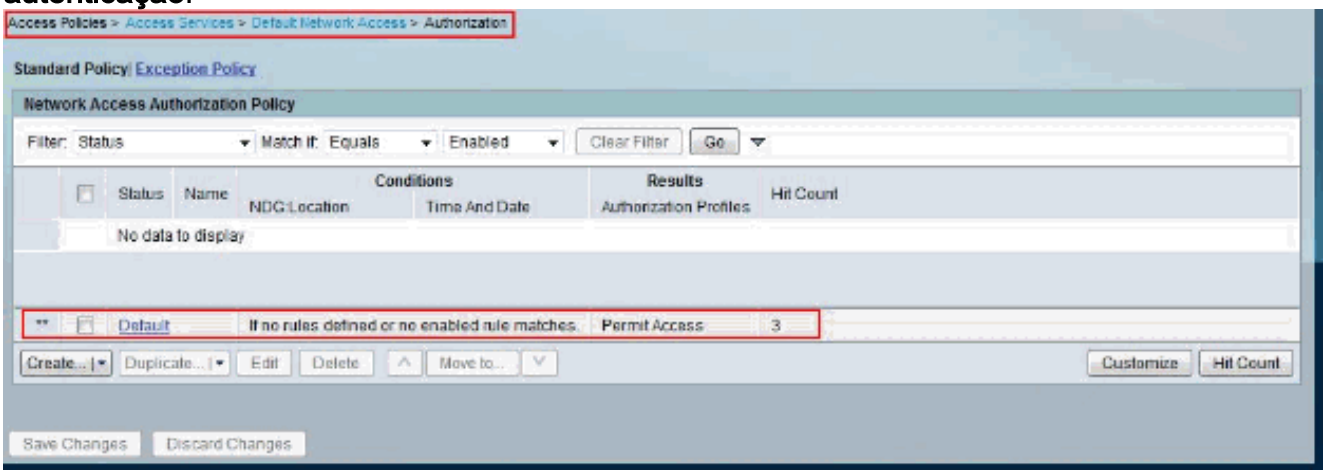
4. Selecione o recém-criado **fixam o servidor ldap** (**myLDAP** neste exemplo), a seguir clicam a **APROVAÇÃO**.



5. Clique **mudanças da salvaguarda**.



6. Vá à seção da **autorização do** serviço identificado em **etapa 1** e assegure-se de que haja pelo menos uma regra que permite a **autenticação**.



Troubleshooting

O ACS envia um pedido do ligamento autenticar o usuário contra um servidor ldap. O pedido do ligamento contém o DN e a senha do usuário do usuário no texto claro. Um usuário for autenticado quando o DN e as compatibilidades de senha do usuário o nome de usuário e senha no diretório LDAP.

- **Erros de autenticação** — O ACS registra erros de autenticação nos arquivos de registro ACS.
- **Erros de inicialização** — Use as configurações de timeout do servidor ldap para configurar o número de segundos que o ACS espera uma resposta de um servidor ldap antes de determinar isso a conexão ou a autenticação nesse server falhou. As razões possíveis para que um servidor ldap retorne um erro de inicialização são:O LDAP não é apoiadoO server está para baixoO server é fora da memóriaO usuário não tem nenhum privilégioAs credenciais incorretas do administrador são configuradas
- **Erros do ligamento** — As razões possíveis para que um servidor ldap retorne erros do ligamento (autenticação) são:Erros de filtraçãoUma busca que usa critérios do filtro falhaErros do parâmetroOs parâmetros inválidos foram incorporadosA conta de usuário é restrita (desabilitado, travado para fora, expirado, a senha expirou, e assim por diante)

Estes erros são registrados como erros dos recursos externos, que indica um problema possível com o servidor ldap:

- Um erro de conexão ocorreu
- O intervalo expirou
- O server está para baixo
- O server é fora da memória

Este erro é registrado como um erro do usuário desconhecido: `Um usuário não existe no base de dados.`

Este erro é registrado como um erro da senha inválida, onde o usuário exista, mas a senha enviada é inválida: `Uma senha inválida foi incorporada.`

Informações Relacionadas

- Cisco Secure Access Control System
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems