ACS 5.x: 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 Cisco Secure Access Control System (ACS) 5.x integra com um base de dados externo LDAP (igualmente chamado uma loja da identidade) usando o protocolo ldap. Há dois métodos usados para conectar ao servidor ldap: texto simples (simples) e conexão SSL (cifrado). O ACS 5.x pode ser configurado para conectar ao servidor ldap usando both of these métodos. Este documento fornece uma configuração de exemplo para conectar o ACS 5.x a um servidor LDAP usando uma conexão simples.

Pré-requisitos

Requisitos

Este documento supõe que o ACS 5.x tem uma conexão IP ao servidor ldap e que a porta TCP 389 está aberta.

Àrevelia, o servidor ldap do microsoft ative directory é configurado para aceitar conexões ldap na

porta TCP 389. Se você está usando qualquer outro servidor ldap, certifique-se de que é em serviço e aceitando conexões na porta TCP 389.

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 aplicativos usados para armazenar e organizar a informação sobre os usuários e os recursos de rede de uma rede de computador. Você pode usar o serviço de diretório a fim controlar o acesso de usuário a estes recursos.

O serviço de diretório LDAP é baseado em um client-server model. Um cliente conecta a um servidor ldap a fim começar uma sessão 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 a fim armazenar 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 chamado 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 a fim 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 a fim 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. Veja o Gerenciamento da conexão ldap.

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 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.

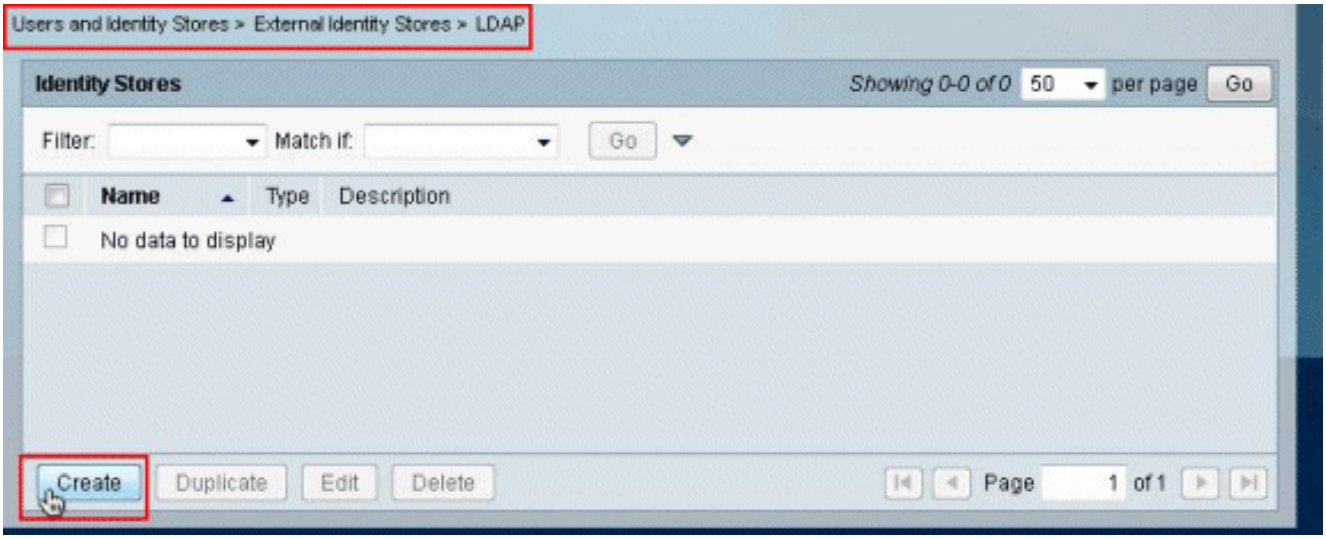
Configurar

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

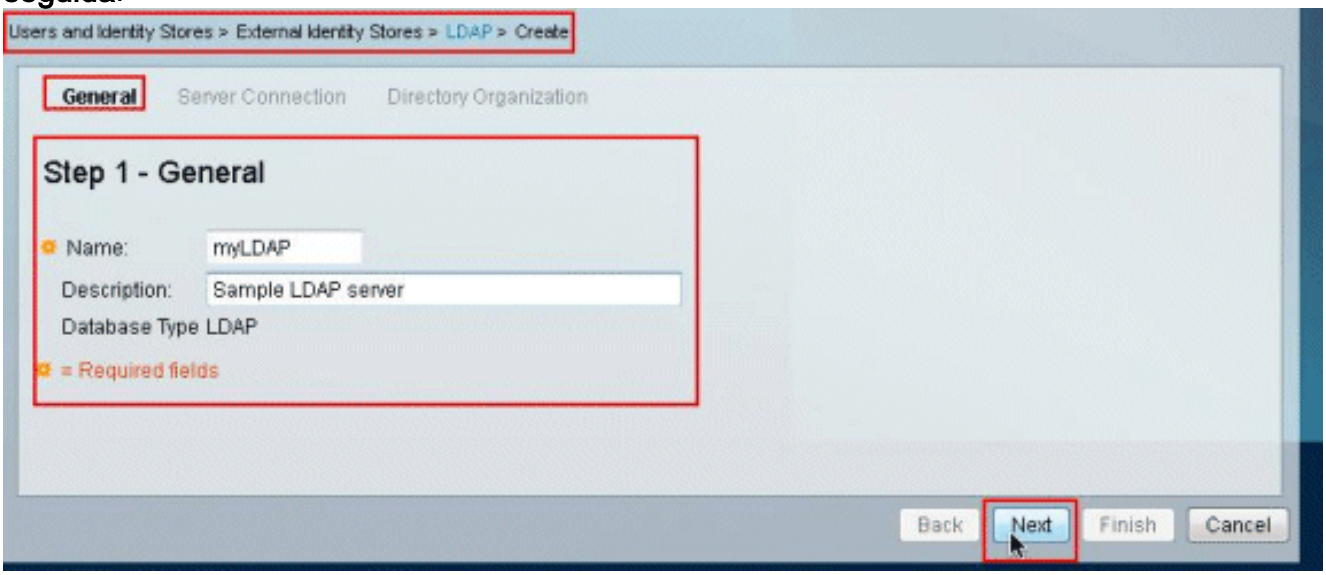
Configurar ACS 5.x para o LDAP

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

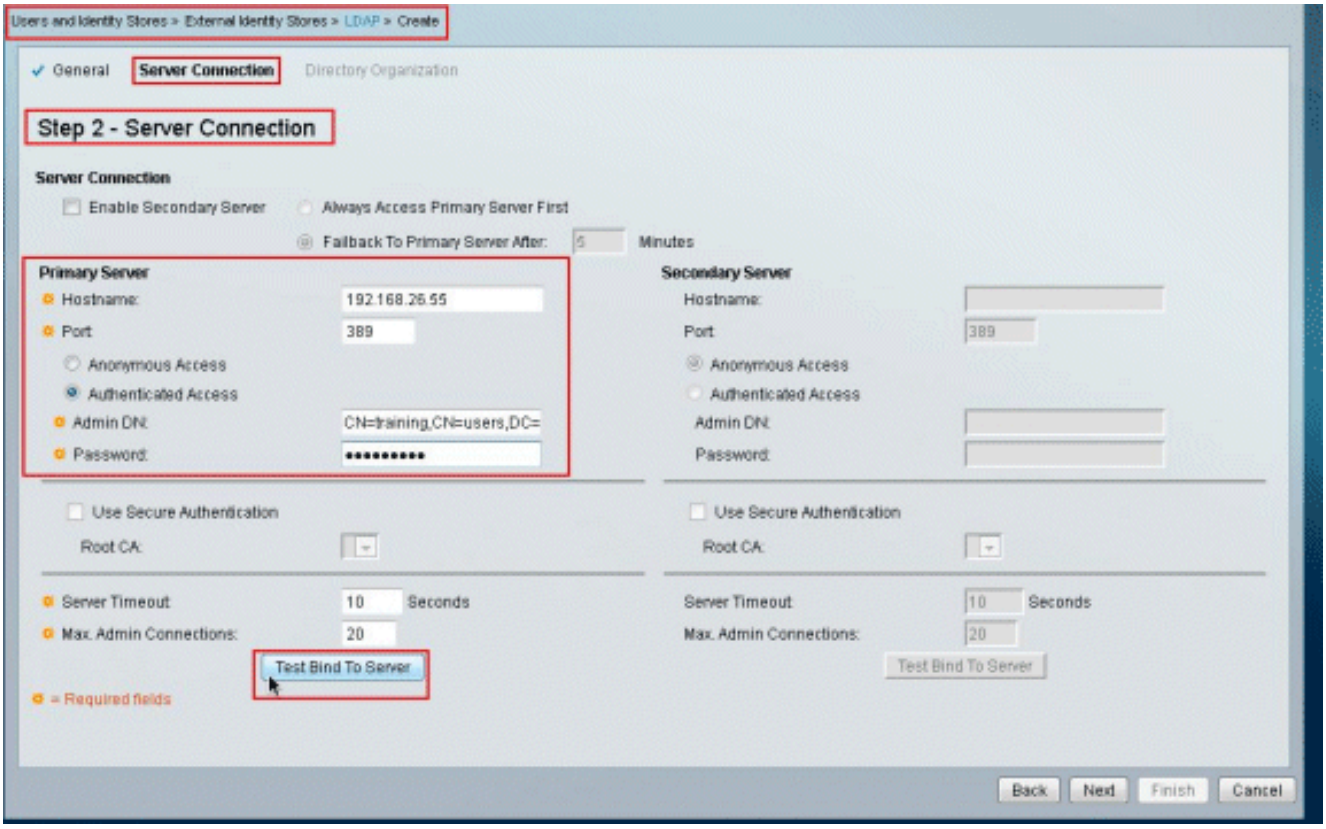
1. Escolha **usuários e a identidade armazena > identidade externo armazena > LDAP**, e o clique **cria** a fim criar uma conexão ldap nova.



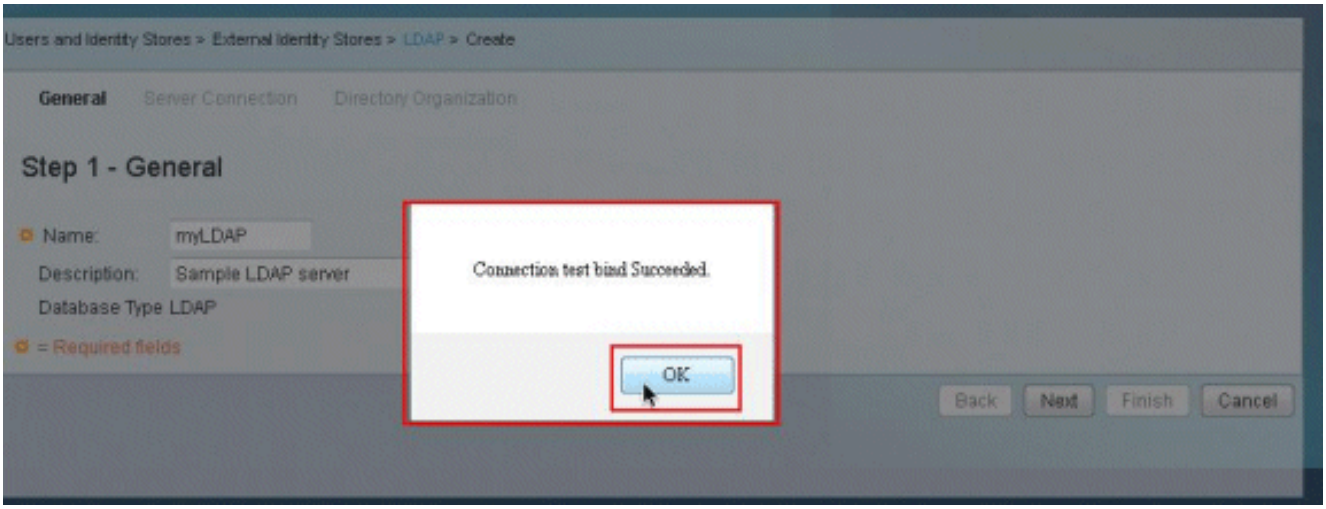
2. No tab geral, forneça o **nome** e a **descrição** (opcionais) para o LDAP novo, e clique-os **em seguida**.



3. Na aba da conexão de servidor sob a seção do servidor primário, forneça o **hostname**, a **porta**, o **Admin DN**, e a **senha**. Clique o **ligamento do teste ao server**.**Nota:** O número de porta atribuído IANA para o LDAP é TCP 389. Contudo, confirme o número de porta que seu servidor ldap está usando de seu LDAP Admin. O Admin DN e senha deve ser-lhe fornecido por seu LDAP Admin. Seu Admin DN deve ter lido todas as permissões em todos os OU no servidor
ldap.

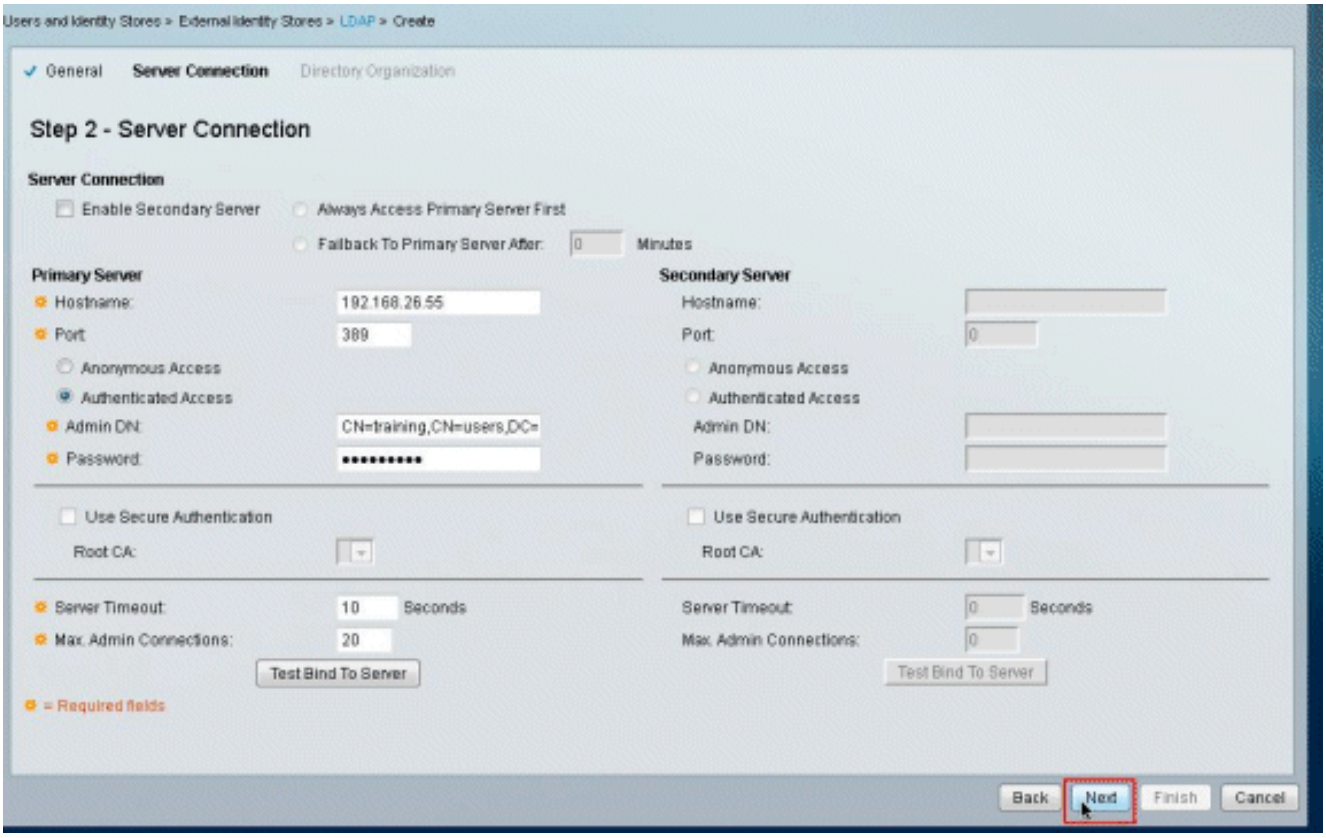


4. Esta imagem mostra que o **ligamento do teste da conexão ao server** era bem sucedido.

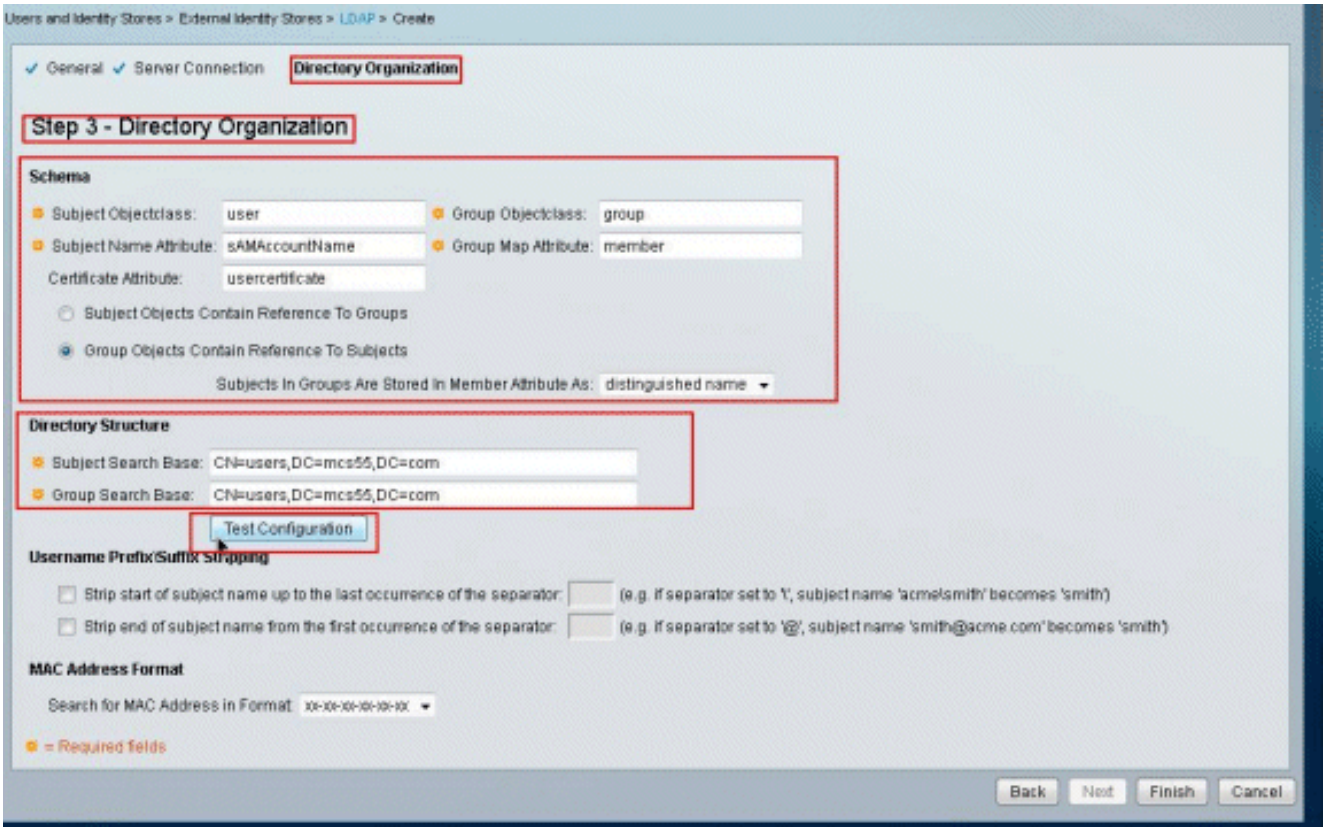


Nota: Se o ligamento do teste não é bem sucedido, re-verifique o **hostname**, o **número de porta**, o **Admin DN**, e a **senha de** seu administrador LDAP.

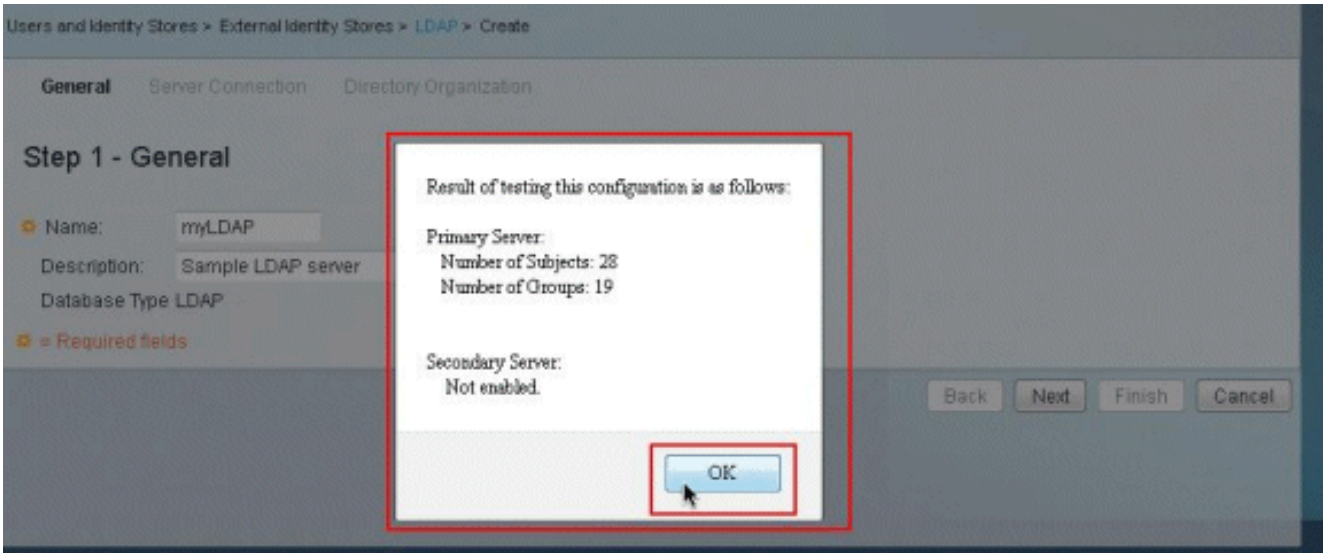
5. Clique em
   Next.



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

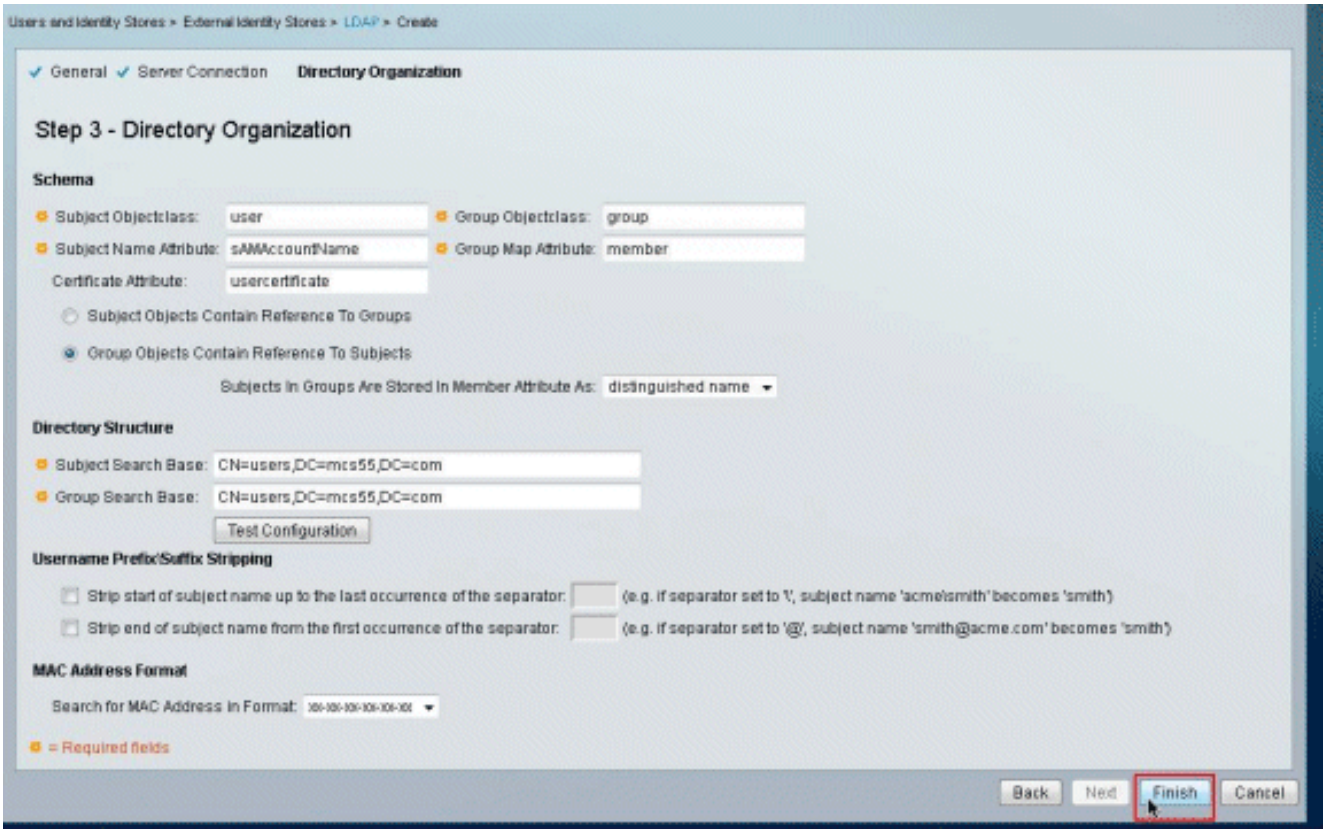


7. Esta imagem mostra que o **teste da configuração** é bem sucedido.

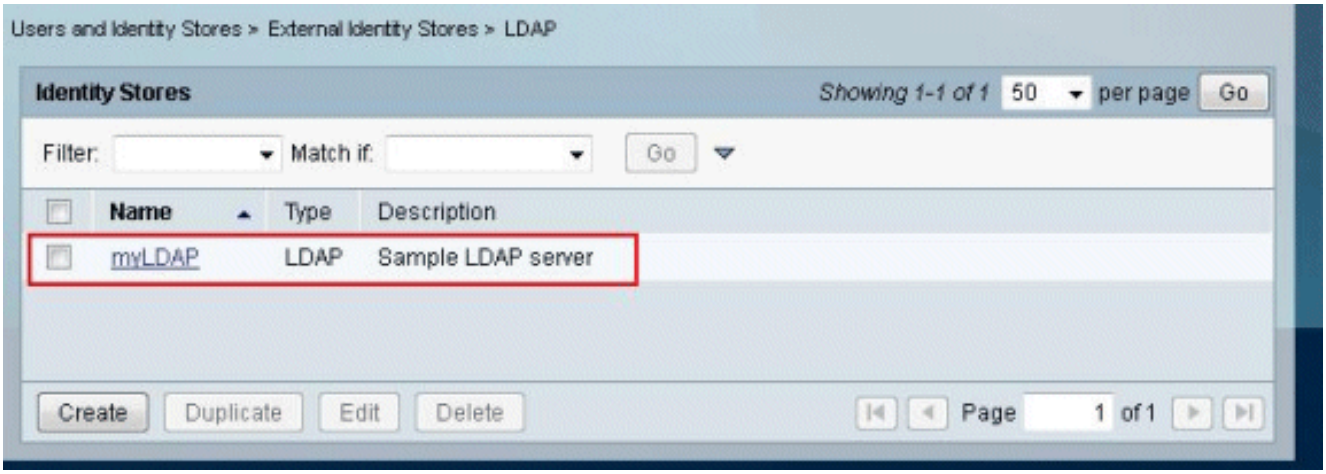


Nota: Se o teste da configuração não é bem sucedido, re-verifique os parâmetros fornecidos no **esquema** e na **estrutura do diretório de** seu administrador LDAP.

8. Clique em
   Finish.



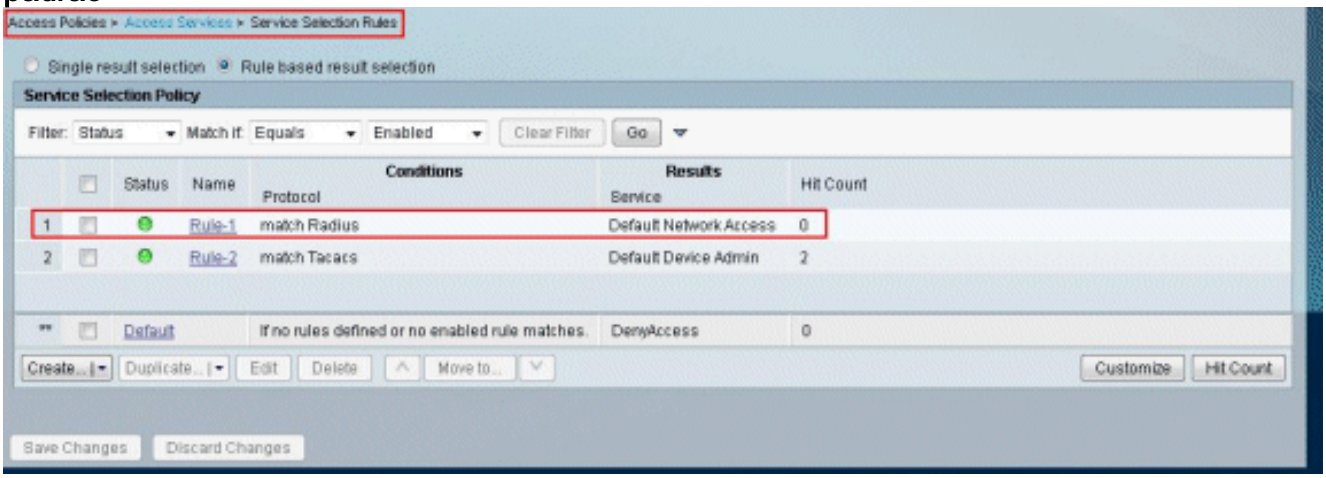
9. **O servidor ldap** é criado com
   sucesso.



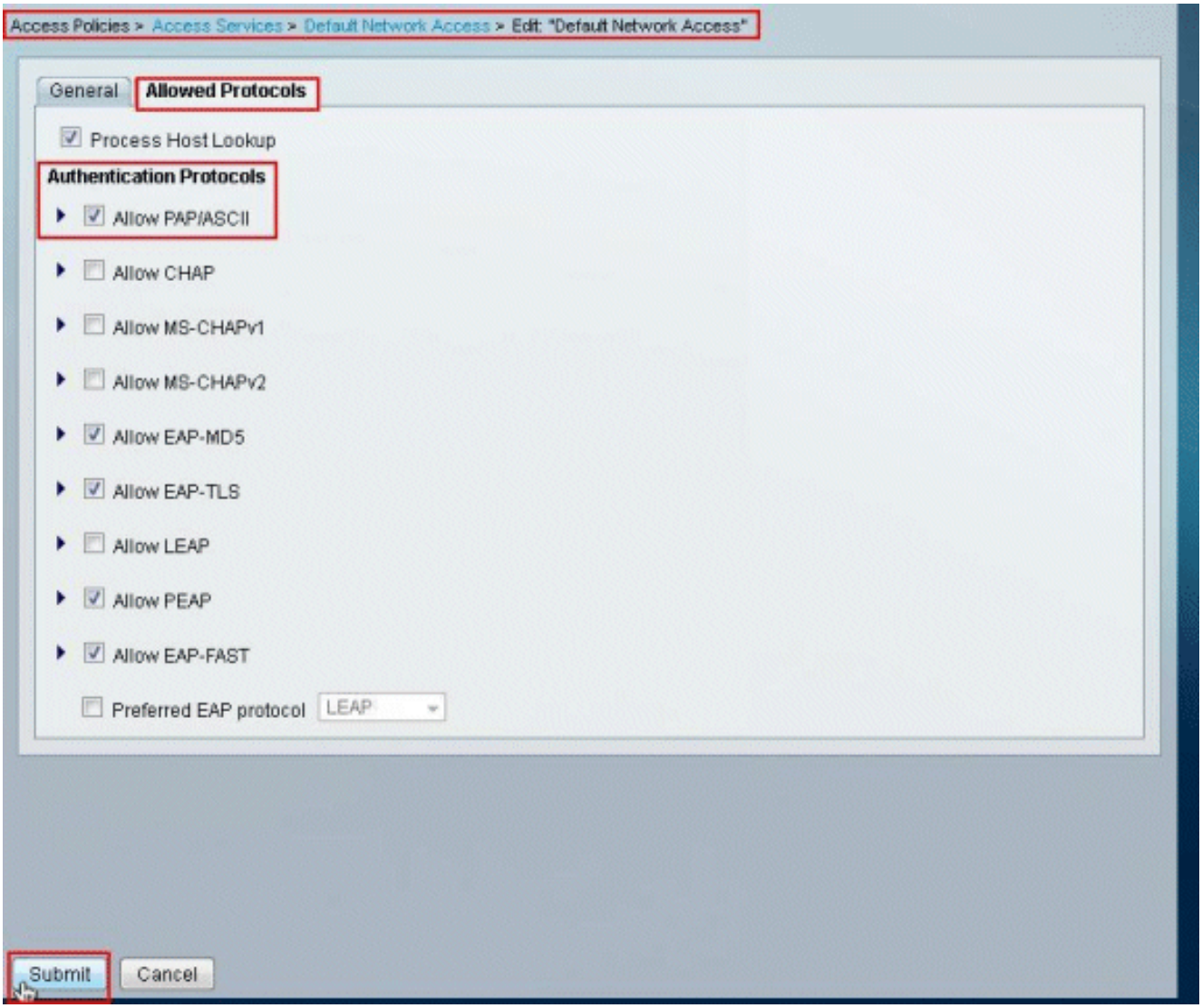
Configurar a loja da identidade

Competem as etapas a fim configurar a loja da identidade:

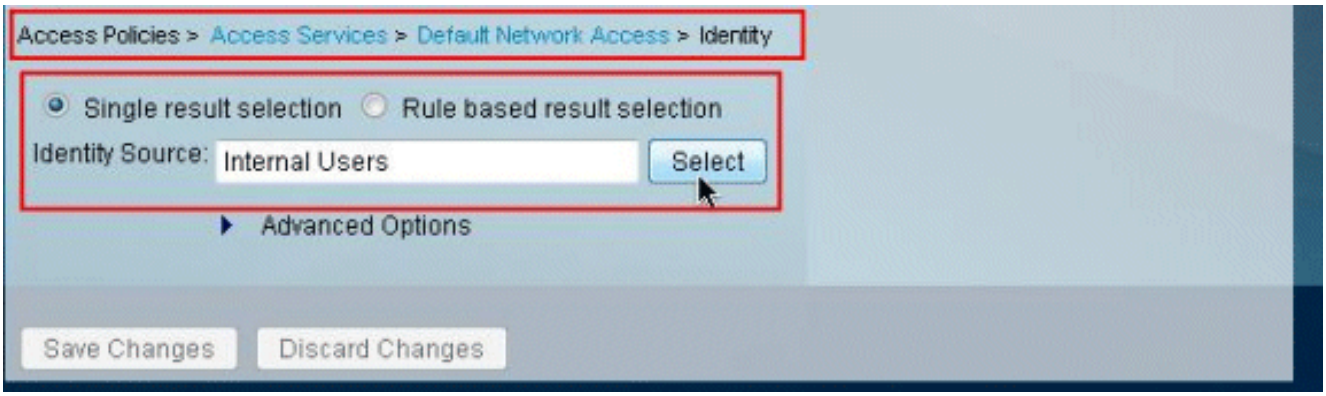
1. Escolha **políticas de acesso > acesso presta serviços de manutenção > regras de seleção do serviço**, e verificam que serviço está indo usar o servidor ldap para a autenticação. Neste exemplo, a autenticação de servidor ldap usa o serviço do **acesso de rede padrão**.



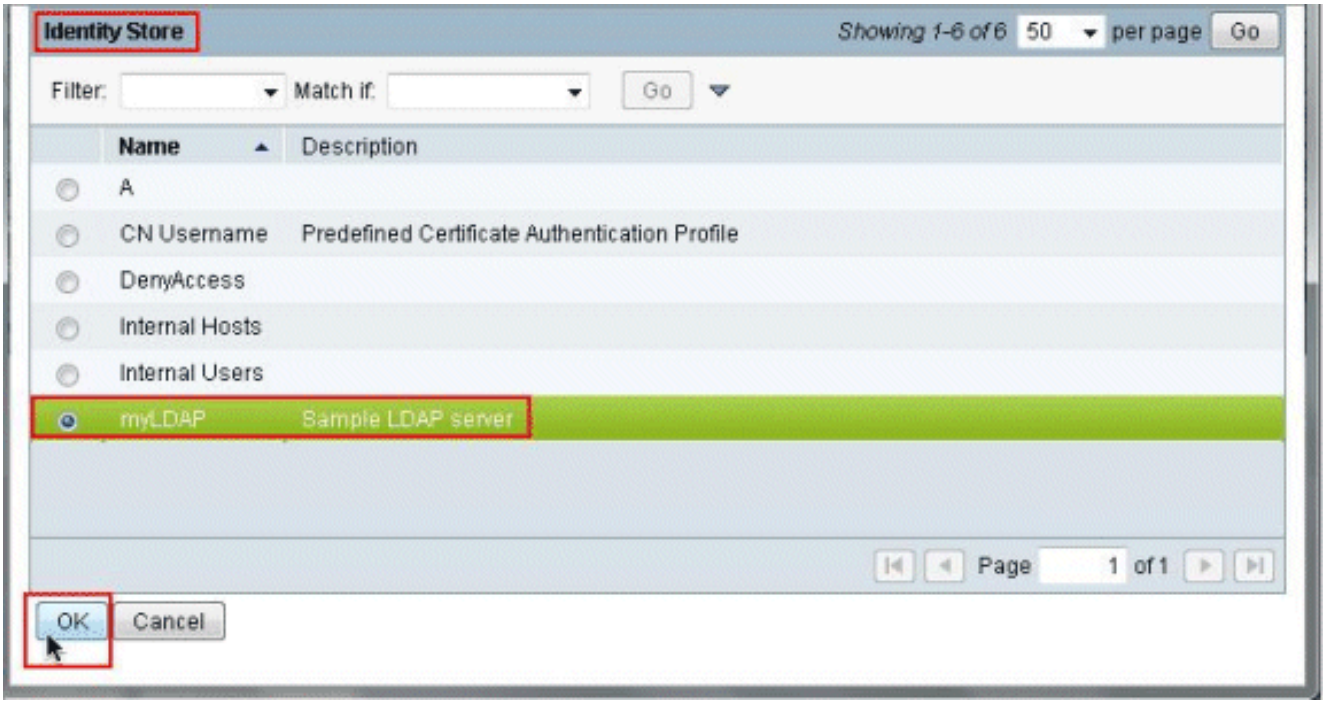
2. Uma vez que você verificou o serviço em etapa 1, vá ao serviço particular e clique **protocolos permitidos**. Certifique-se de que **permita PAP/ASCII** está selecionado, e o clique **se submete**.**Nota:** Você pode ter outros Protocolos de autenticação selecionados junto com para permitir
PAP/ASCII.



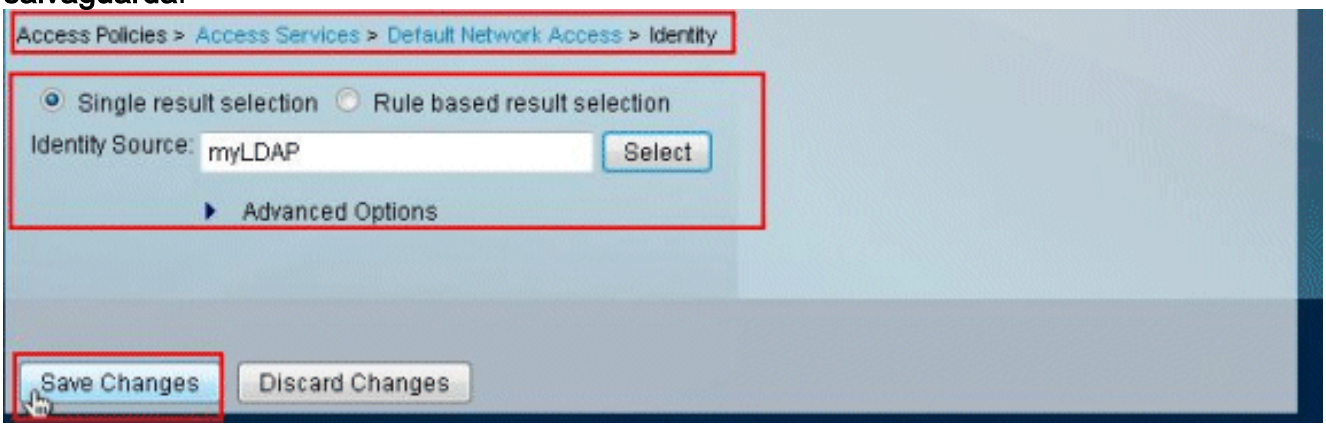
3. Clique sobre o serviço identificado em etapa 1, e clique a **identidade**. Clique **seleto** à direita do campo de fonte da identidade.



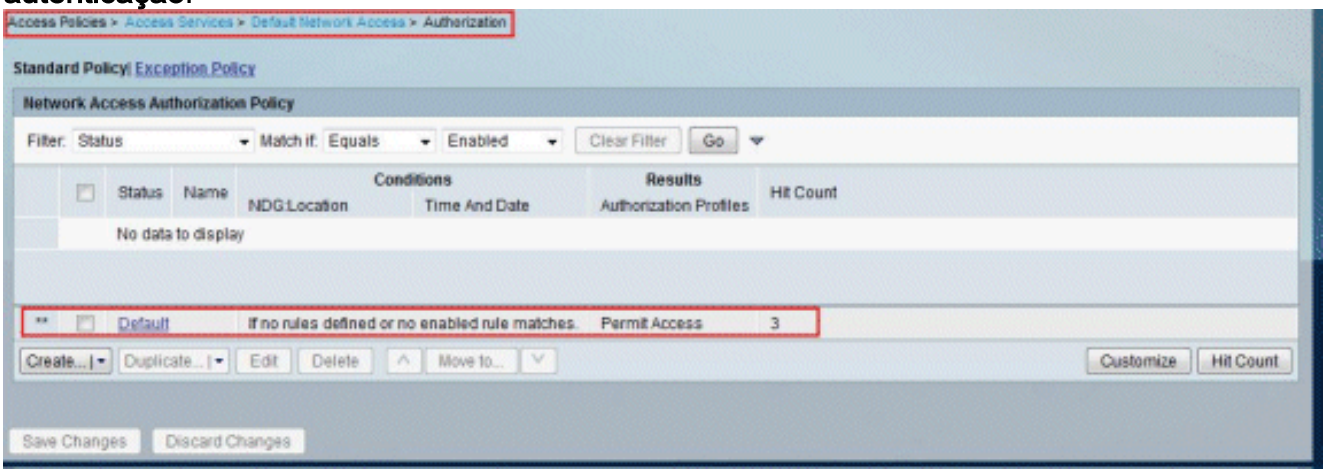
4. Selecione o servidor ldap recém-criado (**myLDAP**, neste exemplo), e clique a **APROVAÇÃO**.



5. Clique **mudanças da salvaguarda**.



6. Vá à seção da autorização do serviço identificado em etapa 1, e certifique-se de que há 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 a fim 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 os erros dos recursos externos, indicando 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

`O usuário A não existe no erro de base de dados` é registrado como um erro do usuário desconhecido.

`Uma senha inválida era` erro `incorporado` é registrada como um erro da senha inválida, onde o usuário existisse, mas a senha enviada é inválida.

Informações Relacionadas

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