ACS 5. x: Пример конфигурации сервера LDAP

Содержание

Введение

Протокол LDAP является сетевым протоколом для того, чтобы запросить и модифицировать сервисы каталогов, которые работают на TCP/IP и UDP. LDAP является легковесным механизмом для доступа к находящемуся в x.500 серверу каталогов. RFC 2251 определяет LDAP.

Система управления доступом Cisco Secure Access Control System (ACS) 5.x интегрируется с внешней базой данных LDAP (также названный идентификационным хранилищем) при помощи Протокола LDAP. Существует два метода, используемые для соединения с Сервером LDAP: (простой) открытый текст и SSL (зашифровал) соединение. ACS 5.x может быть настроен для соединения с Сервером LDAP с помощью обоих из этих методов. Этот документ содержит пример конфигурации для соединения ACS 5.x с сервером LDAP с использованием простого соединения.

Предварительные условия

Требования

Этот документ предполагает, что ACS 5.x имеет IP - подключение к Серверу LDAP и что порт TCP 389 открыт.

По умолчанию Сервер LDAP Microsoft Active Directory настроен для принятия Соединений LDAP на порту TCP 389. При использовании какого-либо другого Сервера LDAP удостоверьтесь, что он подключен и рабочие и принимающие соединения на порту TCP 389.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco Secure ACS 5. x
- Сервер LDAP Microsoft Active Directory

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

Сервис каталогов

Сервис каталогов является программным приложением, или набор приложений использовал хранить и организовывать информацию о пользователях и сетевых ресурсах компьютерной сети. Можно использовать сервис каталогов для управления пользовательским доступом к этим ресурсам.

Сервис каталога LDAP основывается на клиент-серверной модели. Клиент соединяется с Сервером LDAP, чтобы начать сеанс LDAP и отправляет запросы операции к серверу. Сервер тогда передает свои ответы. Один или более Серверов LDAP содержат данные от дерева каталога LDAP или базы данных бэкэнда LDAP.

Сервис каталогов управляет каталогом, который является базой данных, которая содержит информацию. Сервисы каталогов используют распределенную модель, чтобы хранить информацию, и та информация обычно реплицируется между серверами каталогов.

Каталог LDAP организован в простой древовидной иерархии и может быть распределен среди многих серверов. Каждый сервер может иметь реплицированную версию общего каталога, который периодически синхронизируется.

Запись в дереве содержит ряд атрибутов, где каждый атрибут имеет название (тип атрибута или описание атрибута) и одно или более значений. Атрибуты определены в схеме.

Каждая запись имеет уникальный идентификатор, названный его Составным именем (DN). Это название содержит Относительное составное имя (RDN), созданное из атрибутов в записи, придерживавшейся DN родительской записи. Можно думать о DN как о полном имени файла и RDN как относительное имя файла в папке.

Опознавательное Использование LDAP

ACS 5.x может аутентифицировать принципал против идентификационного хранилища LDAP путем выполнения связывать операции на сервере каталогов, чтобы найти и аутентифицировать принципал. Если аутентификация успешно выполняется, ACS может получить группы и атрибуты, которые принадлежат принципалу. Атрибуты для получения могут быть настроены в веб-интерфейсе ACS (страницы LDAP). Эти группы и атрибуты могут использоваться ACS для авторизации принципала.

Чтобы аутентифицировать пользователя или сделать запрос идентификационного хранилища LDAP, ACS соединяется с Сервером LDAP и поддерживает пул соединения. Посмотрите менеджмент Соединения LDAP.

Менеджмент соединения LDAP

ACS 5.x поддерживает множественные параллельные Соединения LDAP. Соединения открыты по требованию во время первой проверки подлинности LDAP. Максимальное число соединений настроено для каждого Сервера LDAP. Вводные соединения заранее сокращают опознавательное время.

Можно заставить максимальное число соединений использовать для параллельных обязательных соединений. Количество открытых соединений может быть другим для каждого Сервера LDAP (основной или вторичный) и определено согласно максимальному числу административных подключений, настроенных для каждого сервера.

ACS сохраняет список открытых Соединений LDAP (включая связывать информацию) для каждого Сервера LDAP, который настроен в ACS. Во время процесса проверки подлинности менеджер подключений пытается найти открытое соединение от пула.

Если открытое соединение не существует, новый открыт. Если Сервер LDAP закрыл соединение, менеджер подключений сообщает, что ошибка во время первого вызова ищет каталог и пытается возобновить соединение.

После того, как процесс проверки подлинности завершен, менеджер подключений освобождает соединение с менеджером подключений. Для получения дополнительной информации обратитесь к ACS 5. X Руководств пользователя.

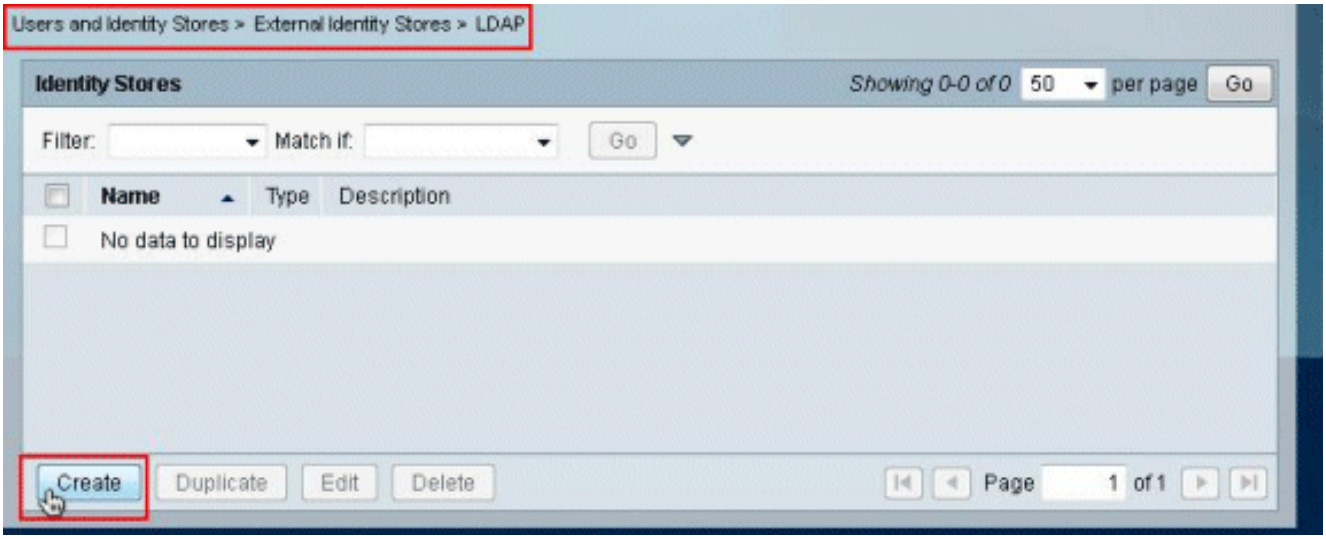
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

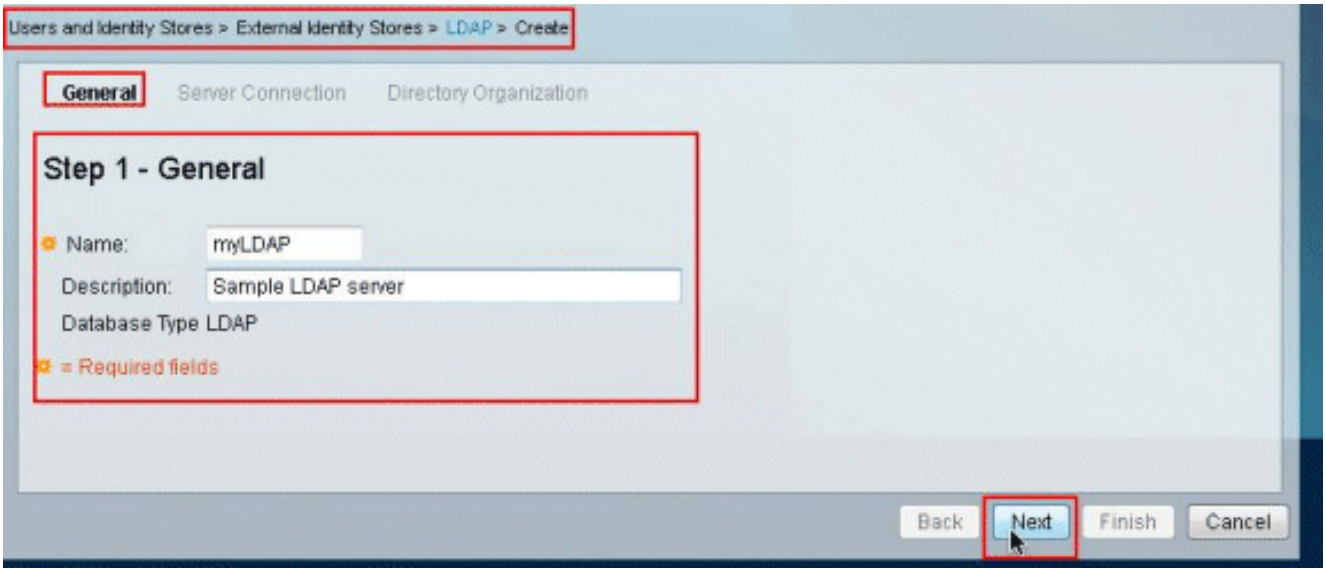
Настройте ACS 5.x для LDAP

Выполните эти шаги для настройки ACS 5.x для LDAP:

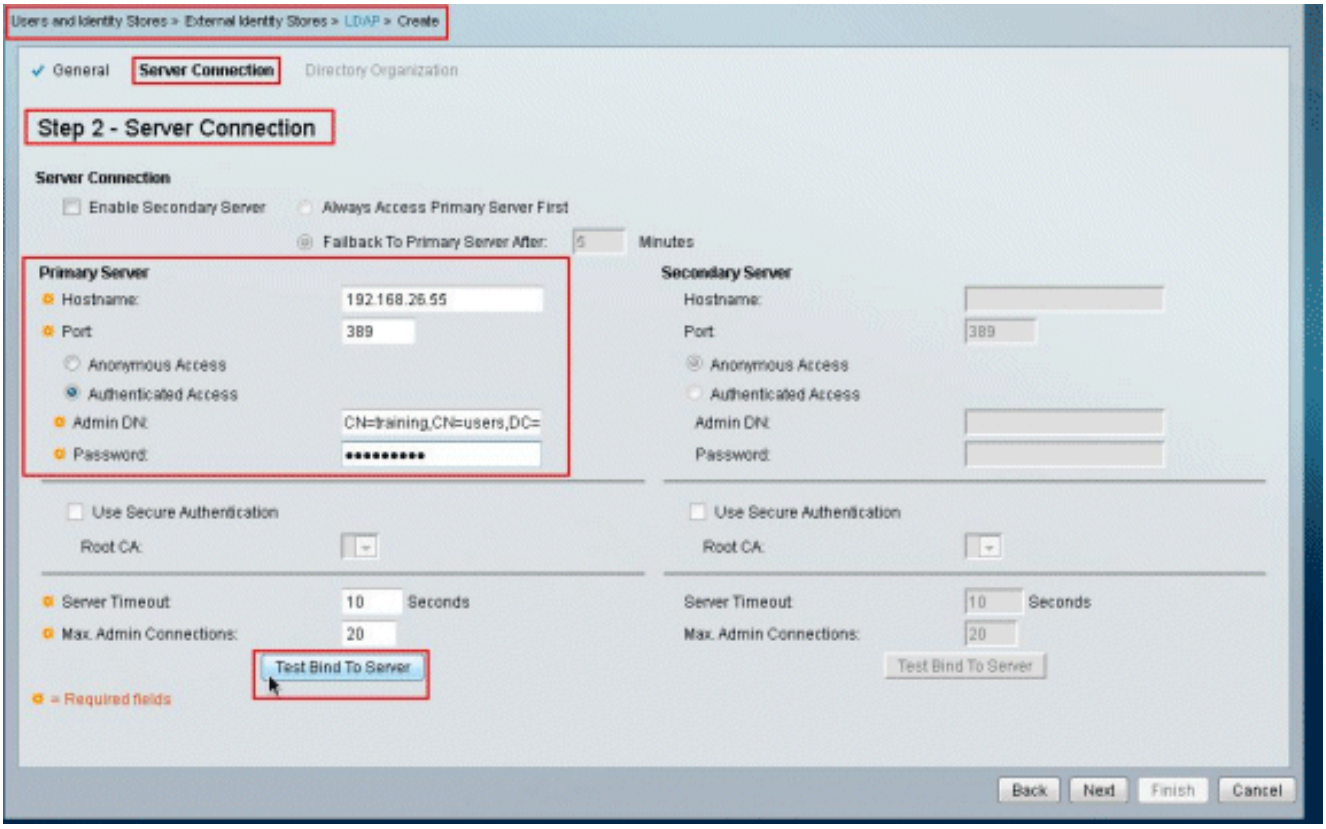
1. Выберите **Users и Identity Stores> External Identity Stores> LDAP**, и нажмите **Create** для создания нового Соединения
   LDAP.



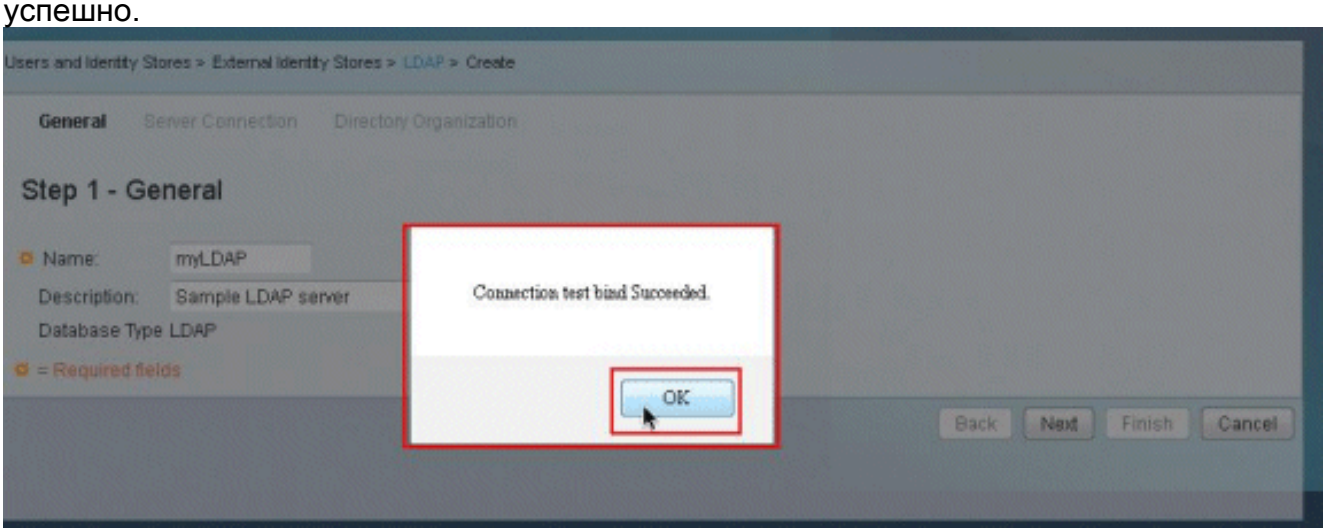
2. Во Вкладке Общие предоставьте **Название** и **Описание** (дополнительное) для нового LDAP, и нажмите
Next.



3. Во вкладке Server Connection под разделом Основного сервера предоставьте **Имя хоста**, **порт**, **DN Admin** и **Пароль**. Нажмите **Test Bind To Server**.**Примечание:** Номер назначенного порта IANA для LDAP является TCP 389. Однако подтвердите номер порта, который ваш Сервер LDAP использует от вашего Admin LDAP. DN Admin и Пароль должны быть предоставлены вам вашим Admin LDAP. Ваш DN Admin должен был считать все разрешения на всех OU на Сервере
LDAP.

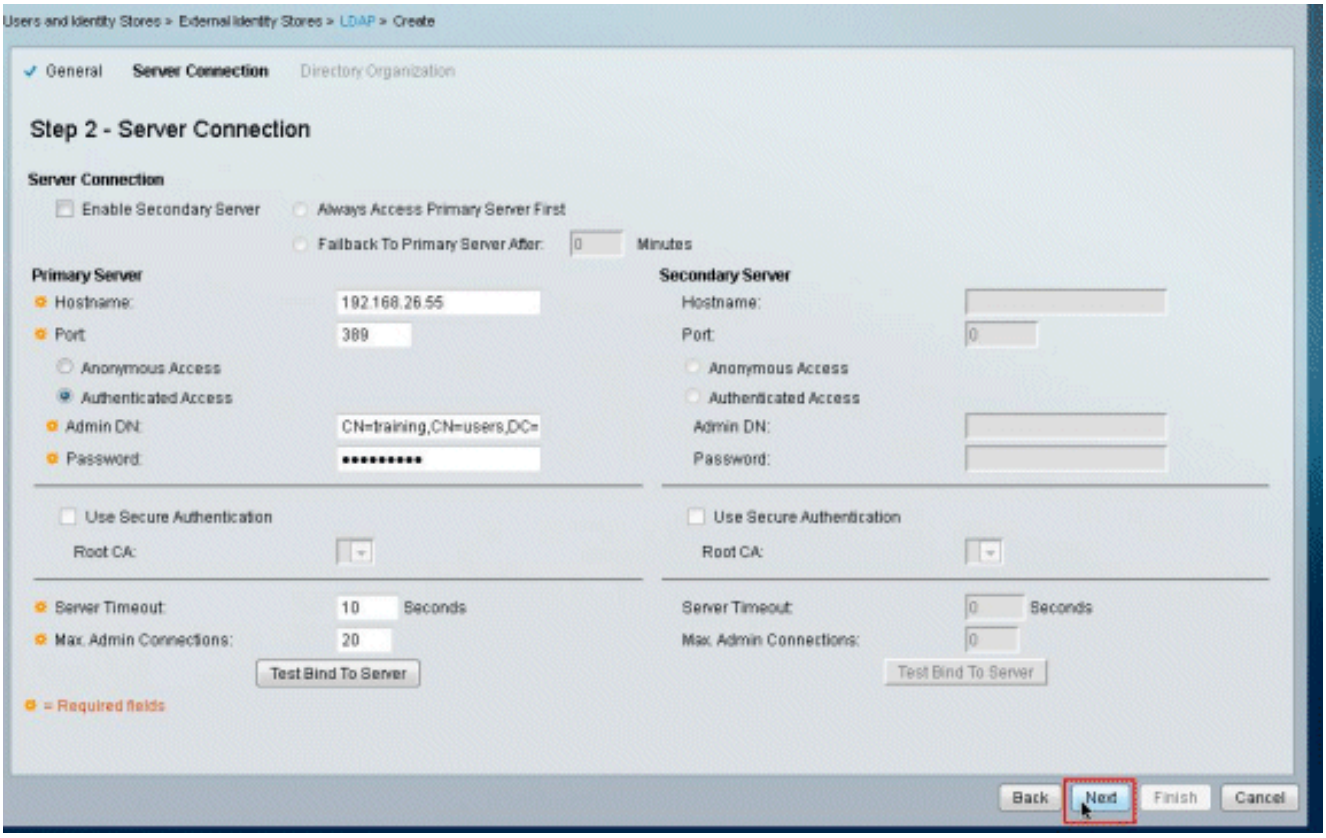


4. Этот образ показывает, что **Тест соединения Связывает с сервером**, было успешно.

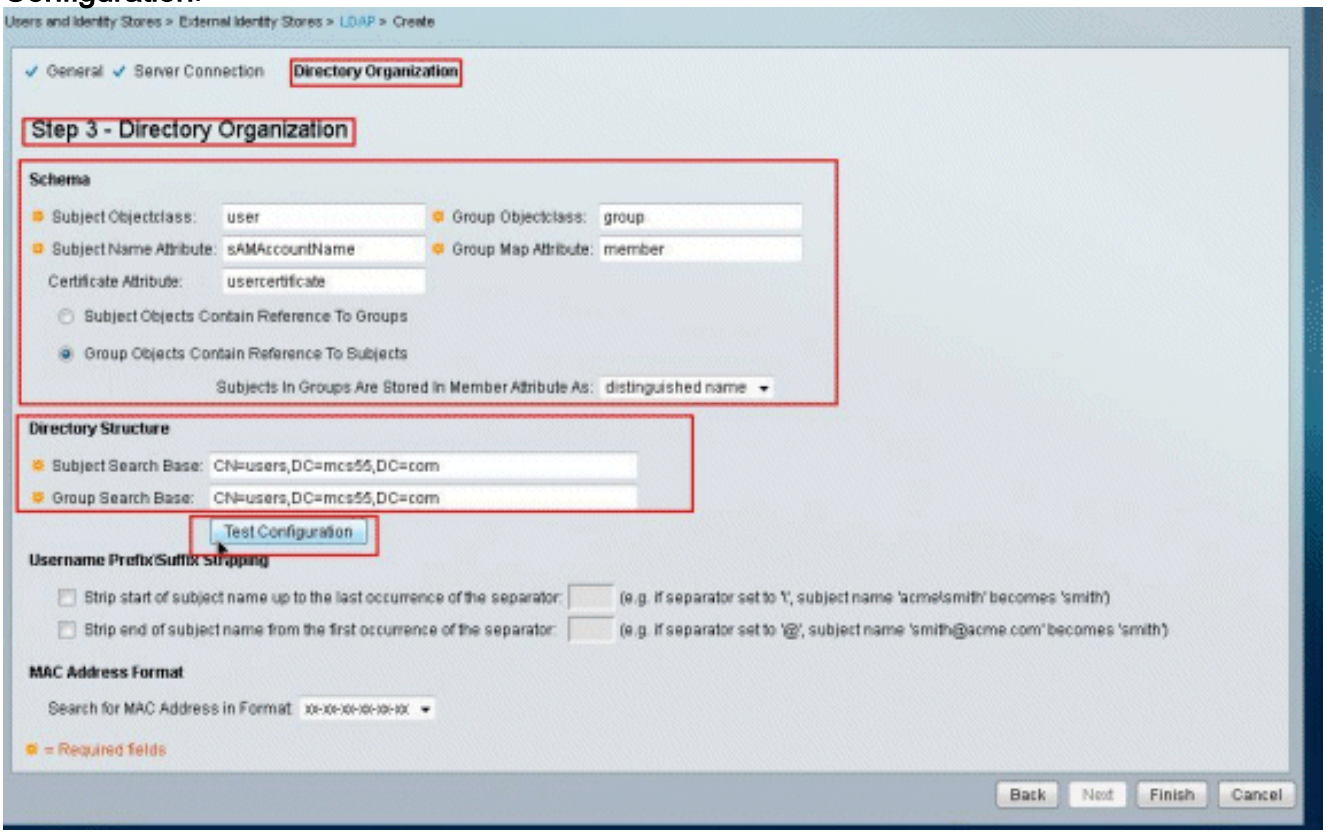


Примечание: Если Тест Связывает, не успешно, повторно проверьте **Имя хоста**, **Номер порта**, **DN Admin** и **Пароль** от вашего Администратора LDAP.

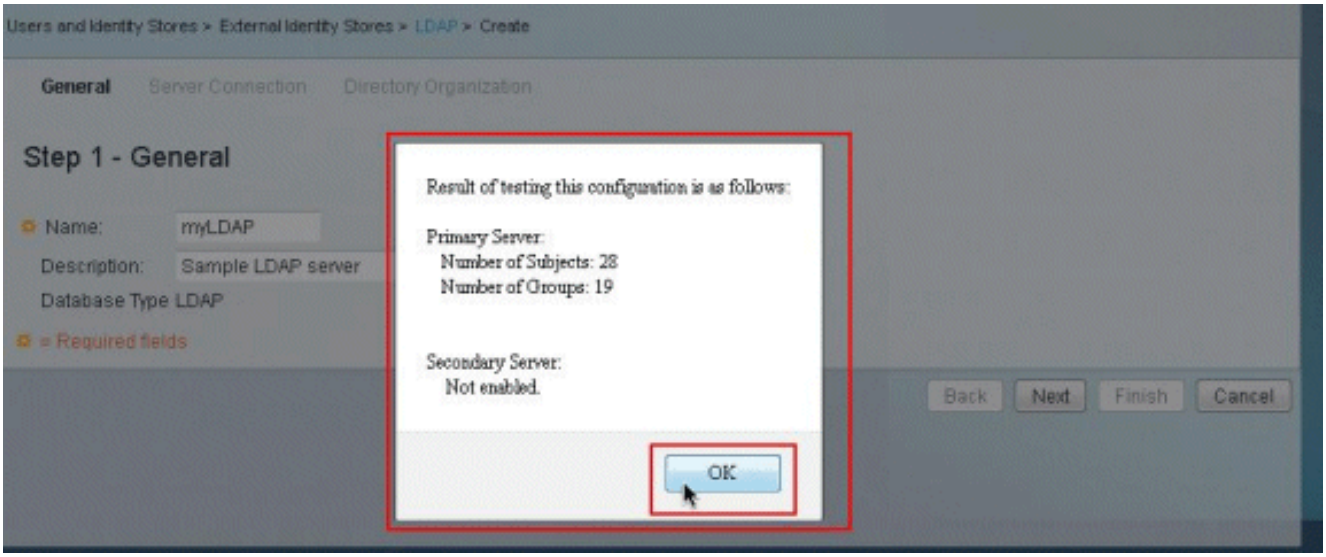
5. **Нажмите кнопку**
   Next.



6. Предоставьте требуемую подробную информацию во вкладке Directory Organization под разделом Схемы. Точно так же предоставьте необходимую информацию под разделом Структуры каталогов в соответствии с вашим Admin LDAP. Нажмите **Test Configuration**.

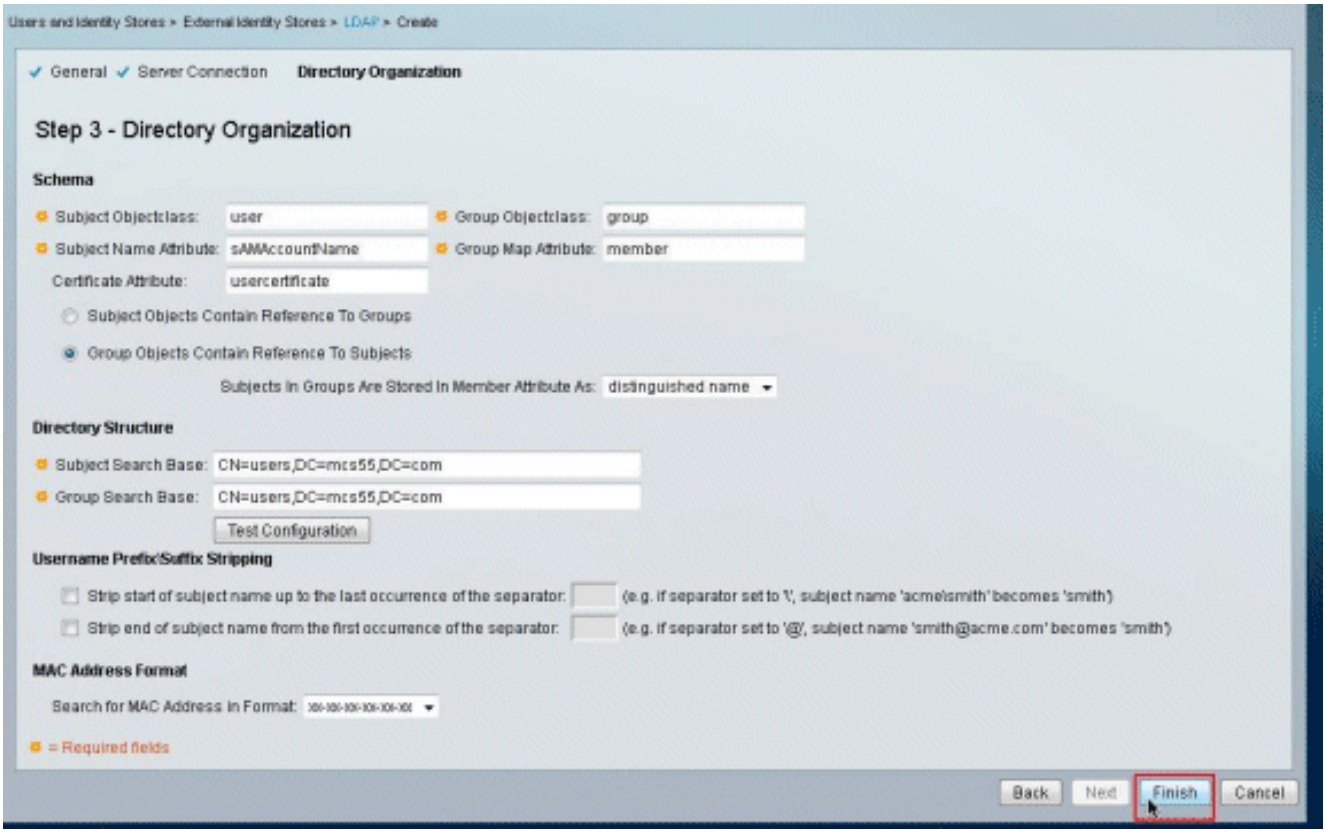


7. Этот образ показывает, что **Конфигурационное испытание** успешно.

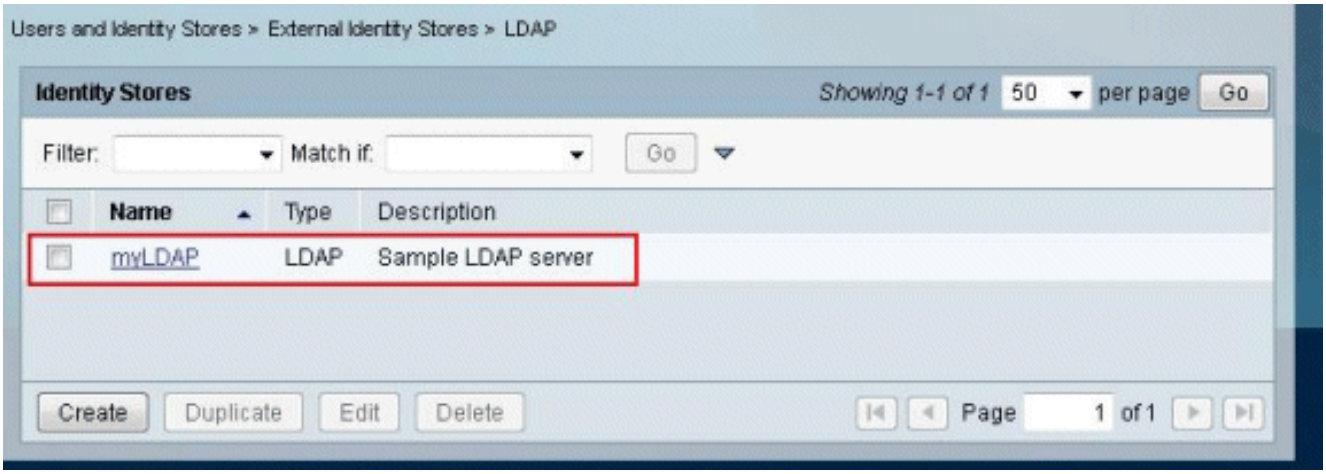


Примечание: Если Конфигурационное испытание не успешно, повторно проверьте параметры, предоставленные в **Схеме** и **Структуре каталогов** от вашего Администратора LDAP.

8. **Нажмите кнопку Finish.**



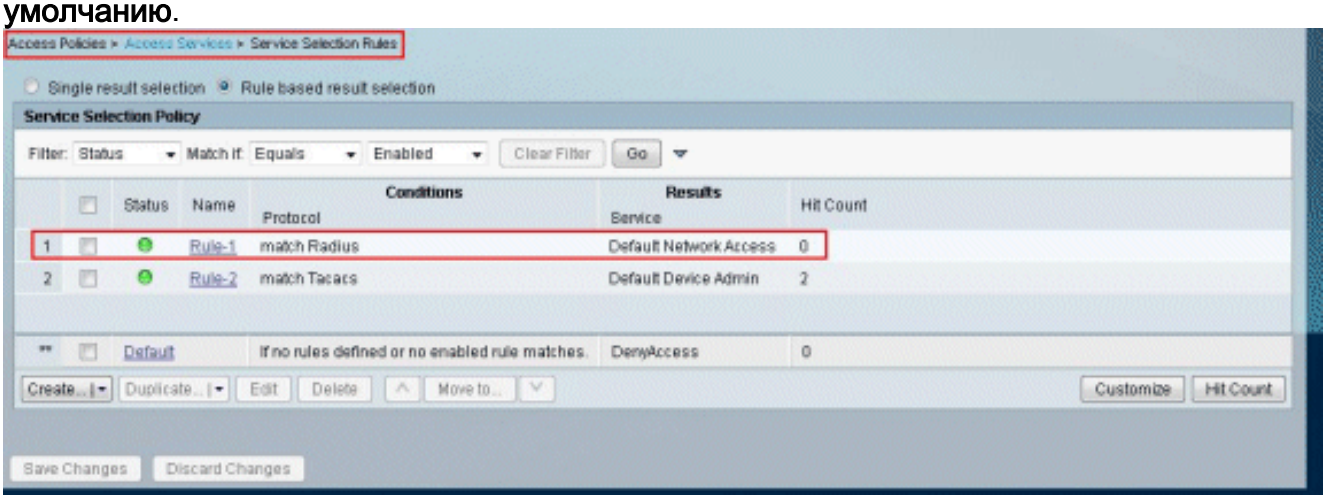
9. **Сервер LDAP** создан успешно.



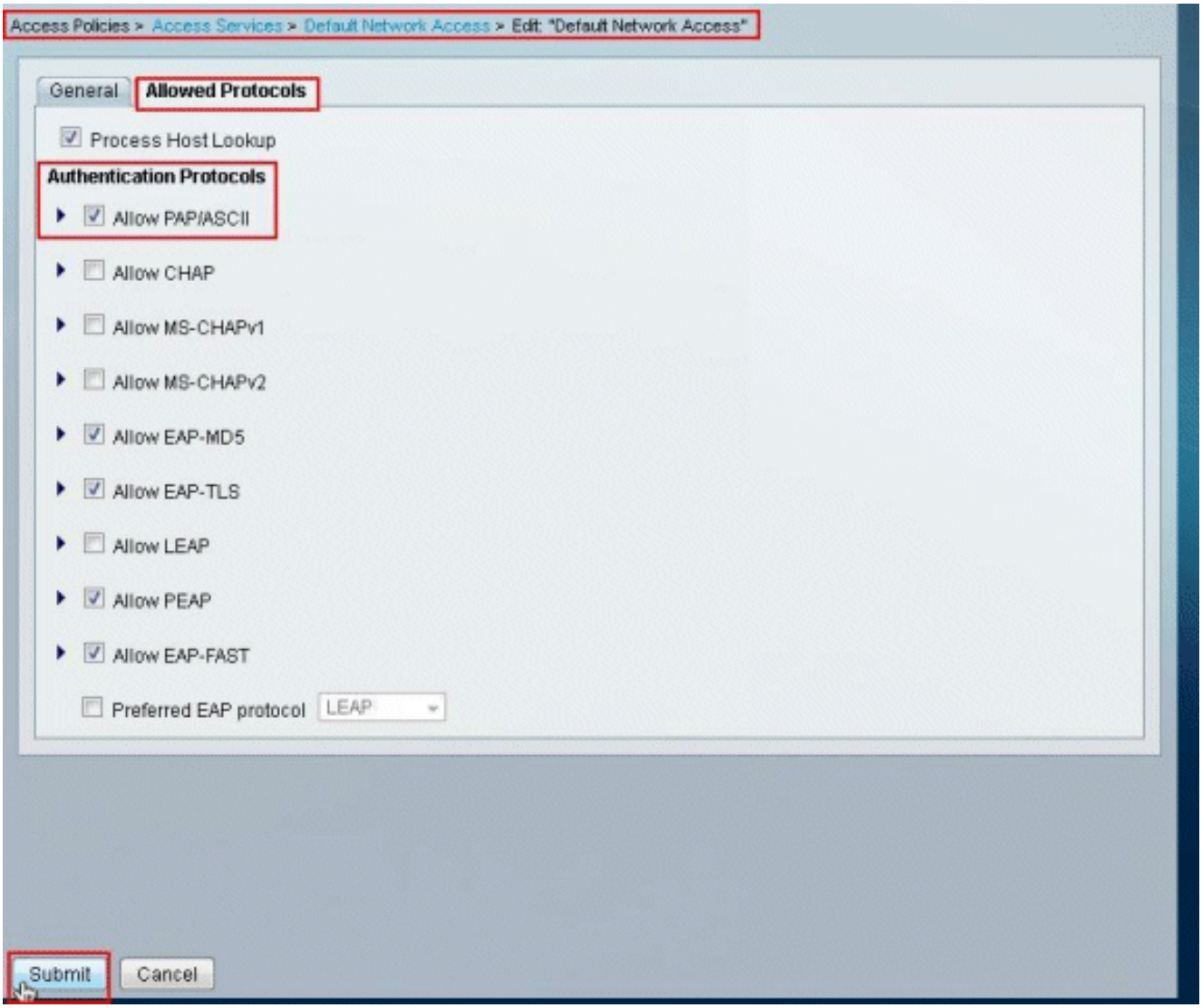
Настройте идентификационное хранилище

Конкурируйте шаги для настройки Идентификационного Хранилища:

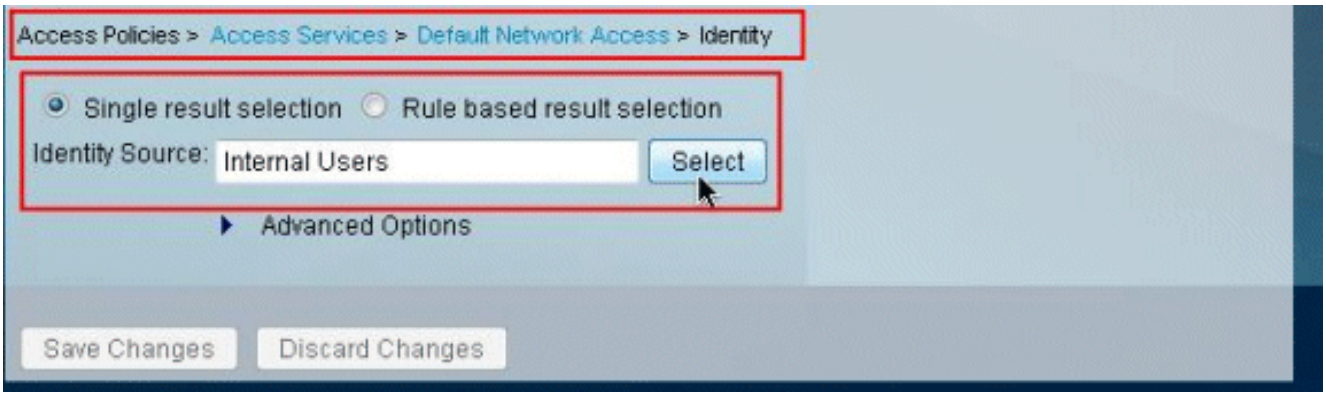
1. Выберите **Access Policies> Access Services> Service Selection Rules** и проверьте, к которому переходит сервис, используют Сервер LDAP для Аутентификации. В данном примере Аутентификация Сервера LDAP использует сервис **Доступа к сети по умолчанию**.



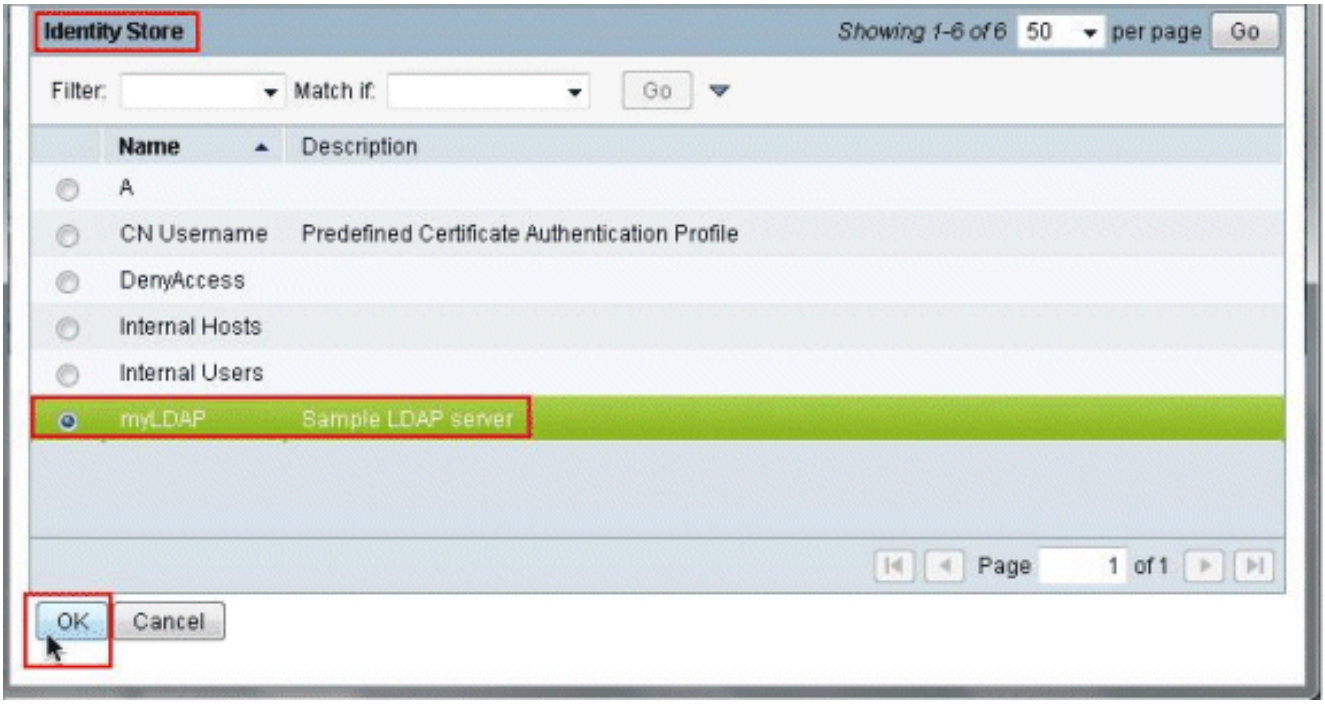
2. Как только вы проверили сервис в Шаге 1, переходите к определенному сервису и нажимаете **Allowed Protocols**. Удостоверьтесь, что **Позволяют, что PAP/ASCII** выбран, и нажмите **Submit**.**Примечание:** Можно было выбрать другие протоколы аутентификации наряду с, Позволяют
PAP/ASCII.



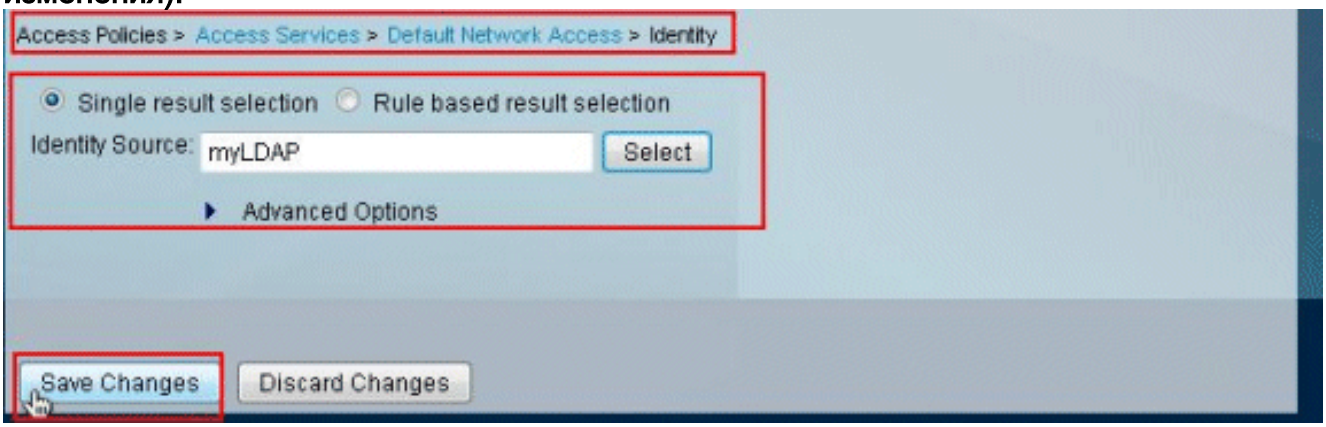
3. Щелкните по сервису, определенному в Шаге 1, и нажмите **Identity**. Нажмите **Select** направо от поля Identity
Source.



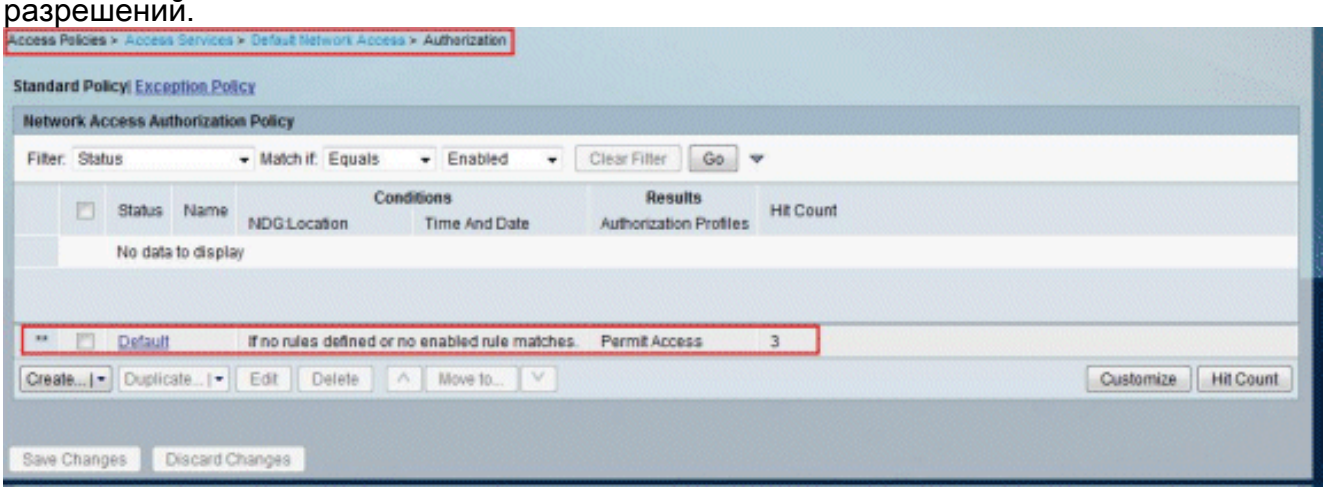
4. Выберите недавно созданный Сервер LDAP (**myLDAP**, в данном примере), и нажмите **OK**.



5. **Нажмите кнопку Save Changes (Сохранить изменения).**



6. Перейдите к разделу Авторизации сервиса, определенного в Шаге 1, и удостоверьтесь, что существует по крайней мере одно Правило что **Аутентификация** разрешений.



Устранение неполадок

ACS отправляет связывать запрос аутентифицировать пользователя против Сервера LDAP. Связывать запрос содержит DN пользователя и пароль пользователя в открытом тексте.

Пользователь аутентифицируется когда DN и совпадения пароля пользователя имя пользователя и пароль в каталоге LDAP.

- **Ошибки аутентификации** - ACS регистрирует ошибки аутентификации в файлах журнала ACS.
- **Ошибки инициализации** - Использование настройки времени ожидания Сервера LDAP для настройки кол-ва секунд, что ACS ждет ответа от Сервера LDAP прежде, чем решить, что отказали соединение или аутентификация на том сервере. Возможные причины для Сервера LDAP для возврата ошибки инициализации:LDAP не поддерживаетсяСервер не работаетСервер вне памятиУ пользователя нет привилегийНастроены неправильные учетные данные администратора
- **Свяжите Ошибки** - Возможные причины для Сервера LDAP для возврата связывают (опознавательные) ошибки:Ошибки фильтрацииПоиск с помощью сбоев критериев фильтраОшибки параметраНедопустимые параметры были введеныУчетная запись пользователя ограничена (отключенный, заблокированный, истек, пароль истек, и так далее),

Эти ошибки зарегистрированы как ошибки внешнего ресурса, указав на возможную проблему с Сервером LDAP:

- Ошибка подключения произошла
- Таймаут истек
- Сервер не работает
- Сервер вне памяти

Ошибка `A user does not exist in the database` зарегистрирована как ошибка Неизвестного пользователя.

Ошибка `An invalid password was entered` зарегистрирована как ошибка Неверного пароля, где пользователь существует, но передаваемый пароль недопустим.

Дополнительные сведения

- Система управления доступом Cisco Secure Access Control System
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация