ACS 5. X: Безопасный пример конфигурации сервера LDAP

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Общие сведения
Настройка
Установите корневой сертификат CA на ACS 5. x
Настройте ACS 5. X для безопасного LDAP
Настройте идентификационное хранилище
Устранение неполадок
Дополнительные сведения

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.

Access Control Server (ACS) 5.x интегрируется с внешней базой данных LDAP, также названной идентификационным хранилищем, при помощи Протокола LDAP. Существует два метода 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 методы. В этом документе ACS 5.x настроен для соединения с Сервером LDAP с помощью зашифрованного соединения.

Предварительные условия

Требования

Этот документ предполагает, что ACS 5.x имеет IP - подключение к Серверу LDAP, и порт TCP 636 открыт.

Сервер LDAP Active Directory Microsoft® должен быть настроен для принятия безопасных Соединений LDAP на порту TCP 636. Этот документ предполагает, что у вас есть корневой сертификат Центра сертификации (CA), кто выполнил серверный сертификат к Microsoft LDAP server. Для получения дополнительной информации о том, как настроить Сервер

LDAP, обратитесь к тому, Как включить LDAP по SSL со сторонним центром сертификации.

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 рядом приложений, для того, чтобы сохранить и организовать 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 начинает сеанс LDAP путем соединения с Сервером 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 для того, 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: его Составное имя (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.

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

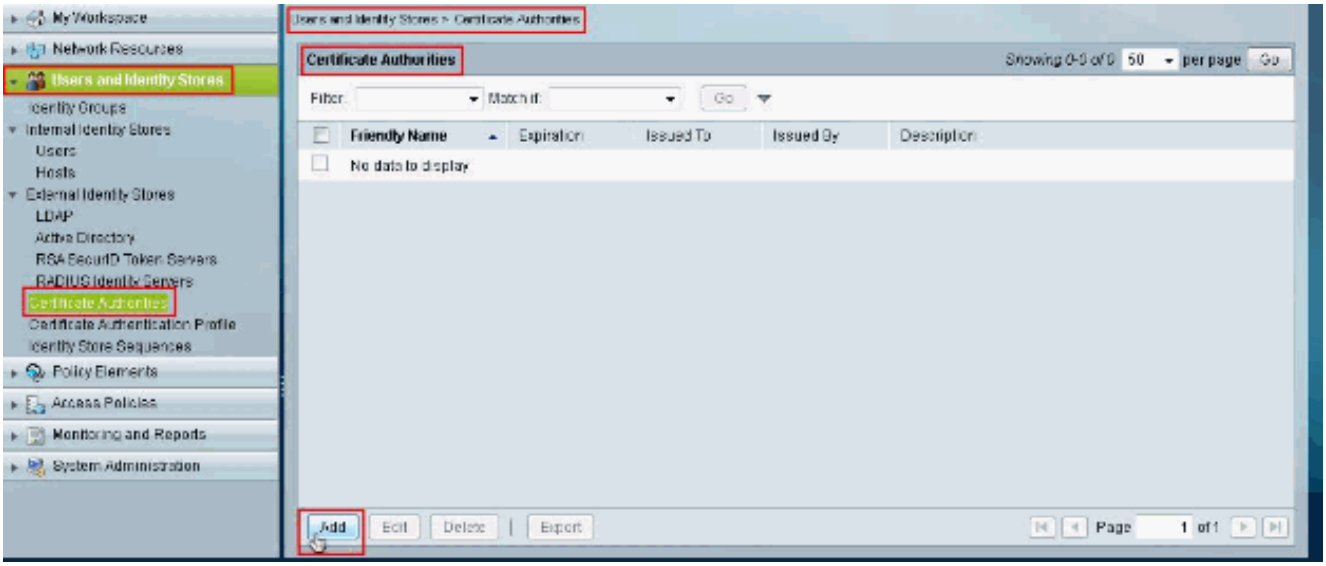
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Установите корневой сертификат CA на ACS 5. x

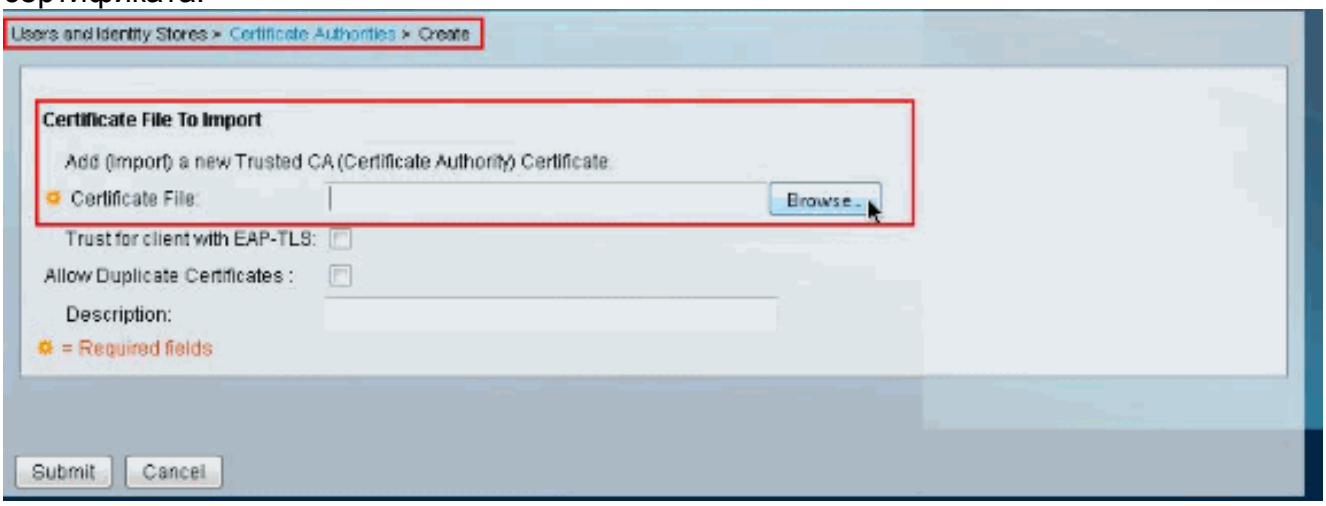
Выполните эти шаги для установки Корневого сертификата CA на Cisco Secure ACS 5. x:

Примечание: Гарантируйте, что Сервер LDAP предварительно сконфигурирован для принятия зашифрованных соединений на порту TCP 636. Для получения дополнительной информации о том, как настроить Microsoft LDAP server, обратитесь к тому, Как включить LDAP по SSL со сторонним центром сертификации.

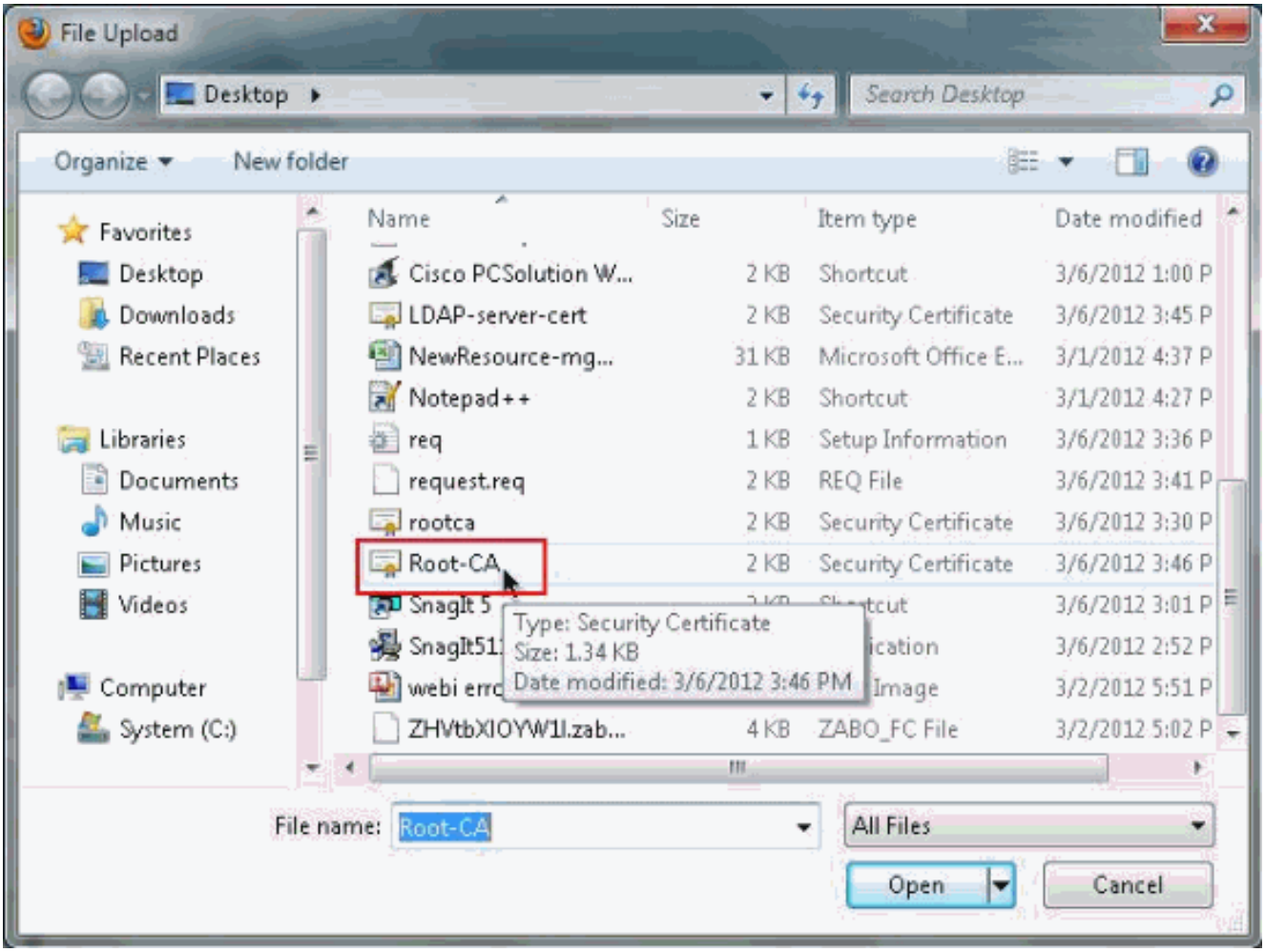
1. Выберите **Users и Identity Stores> Certificate Authorities**, затем **нажмите Add** для добавления корневого сертификата CA, кто выполнил серверный сертификат к Microsoft LDAP
   server.



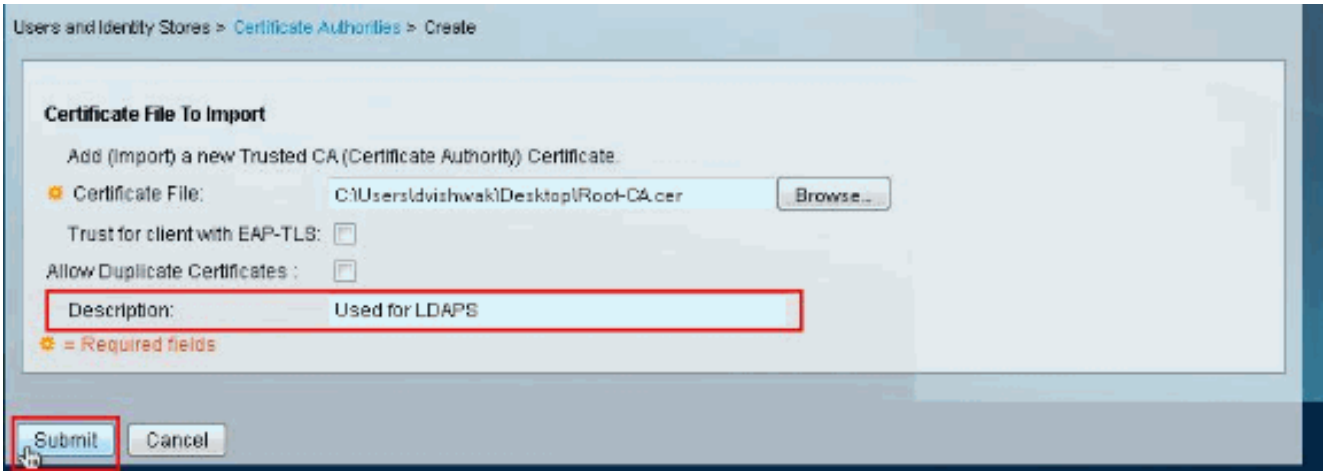
2. От **Файла сертификата для Импорта** раздела нажмите **Browse**, следующий за **Файлом сертификата** для поиска Файла сертификата.



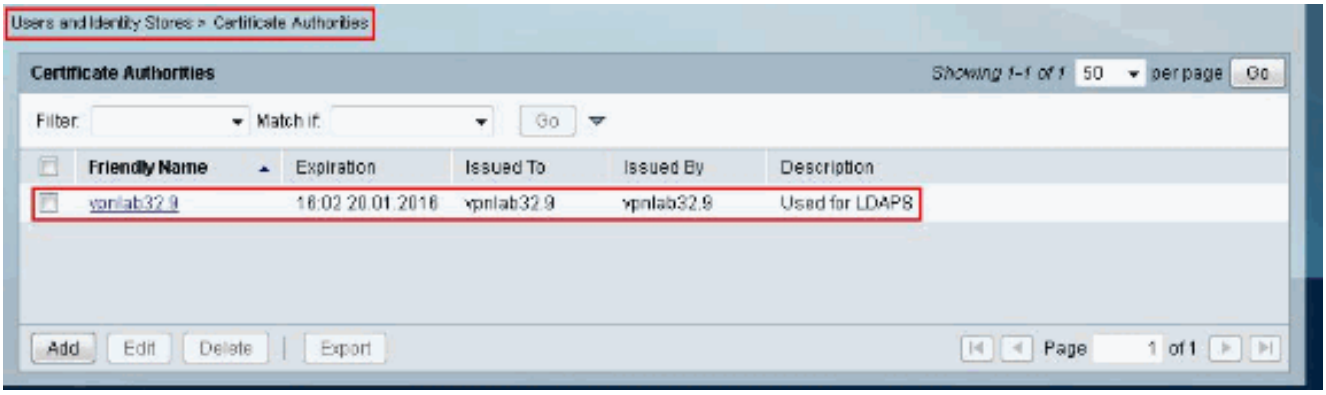
3. Выберите требуемый **Файл сертификата** (корневой сертификат CA, кто выполнил серверный сертификат к Microsoft LDAP server), и нажмите **Open**.



4. Предоставьте **Описание** в пространстве, предоставленном следующий за Описанием, и нажмите
Submit.



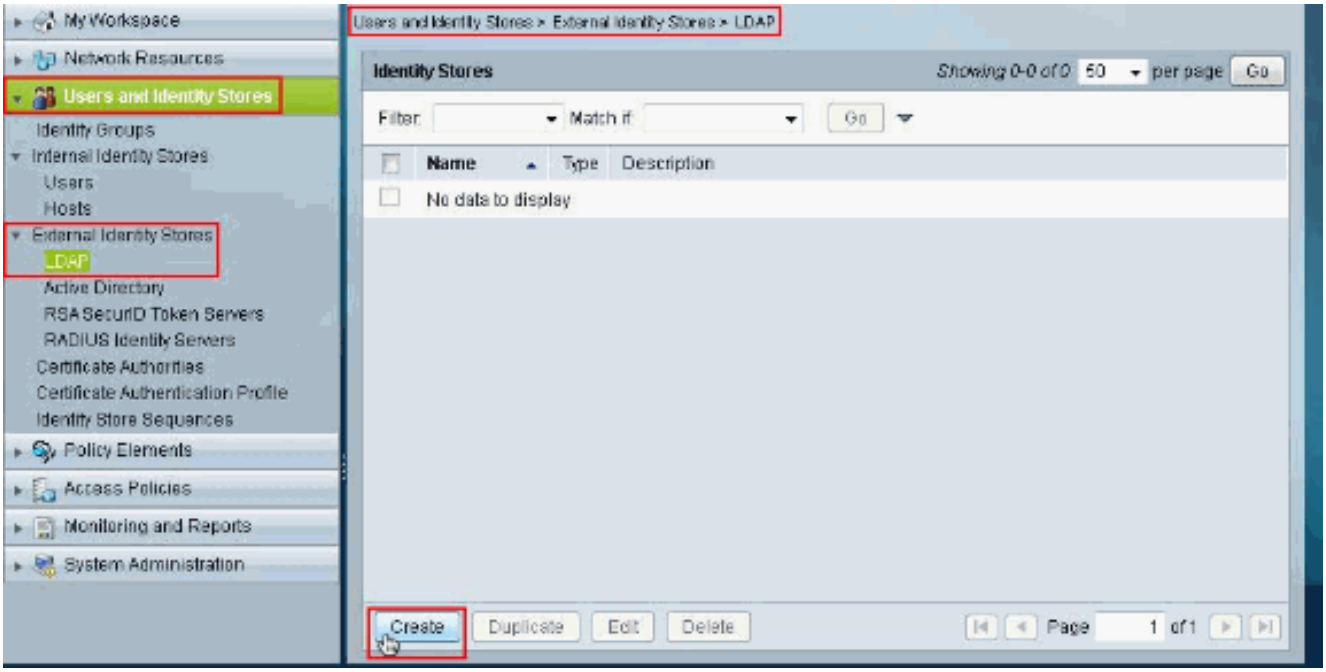
Этот образ показывает, что был должным образом установлен Корневой сертификат:



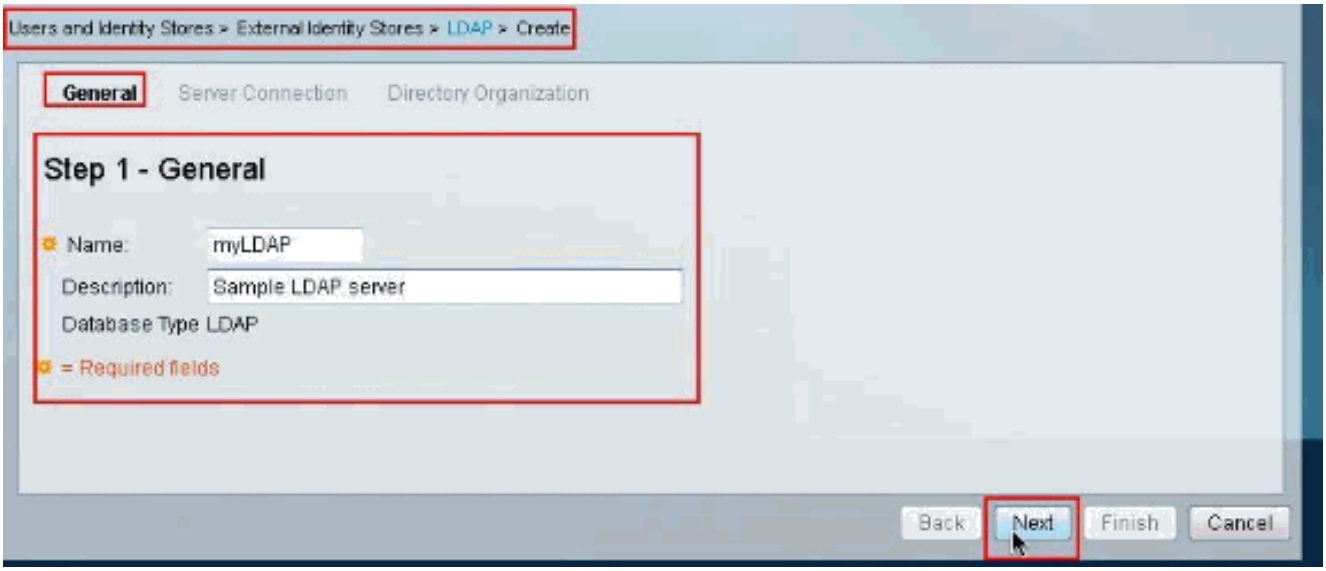
Настройте ACS 5. X для безопасного LDAP

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

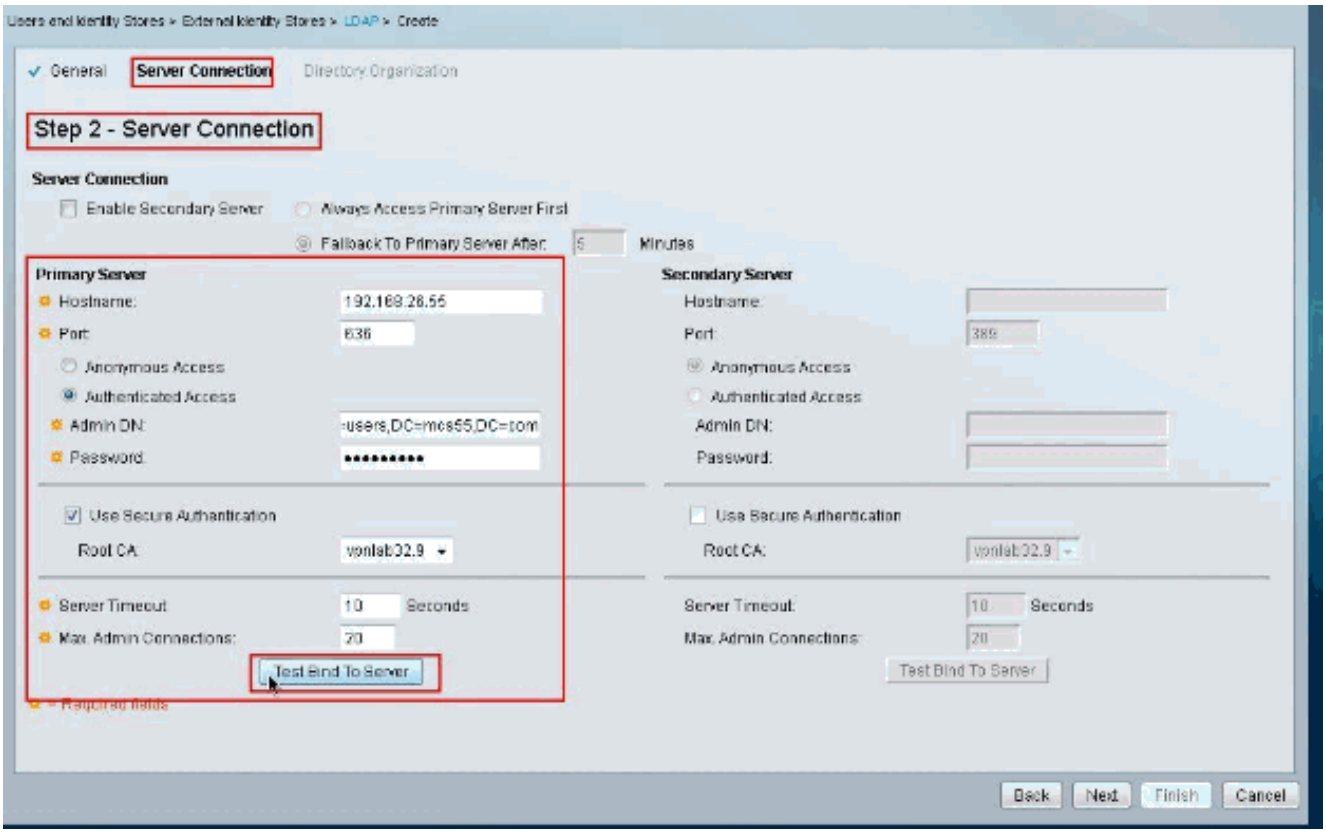
1. Выберите **Users и Identity Stores> External Identity Stores> LDAP** и нажмите **Create** для создания нового Соединения
   LDAP.



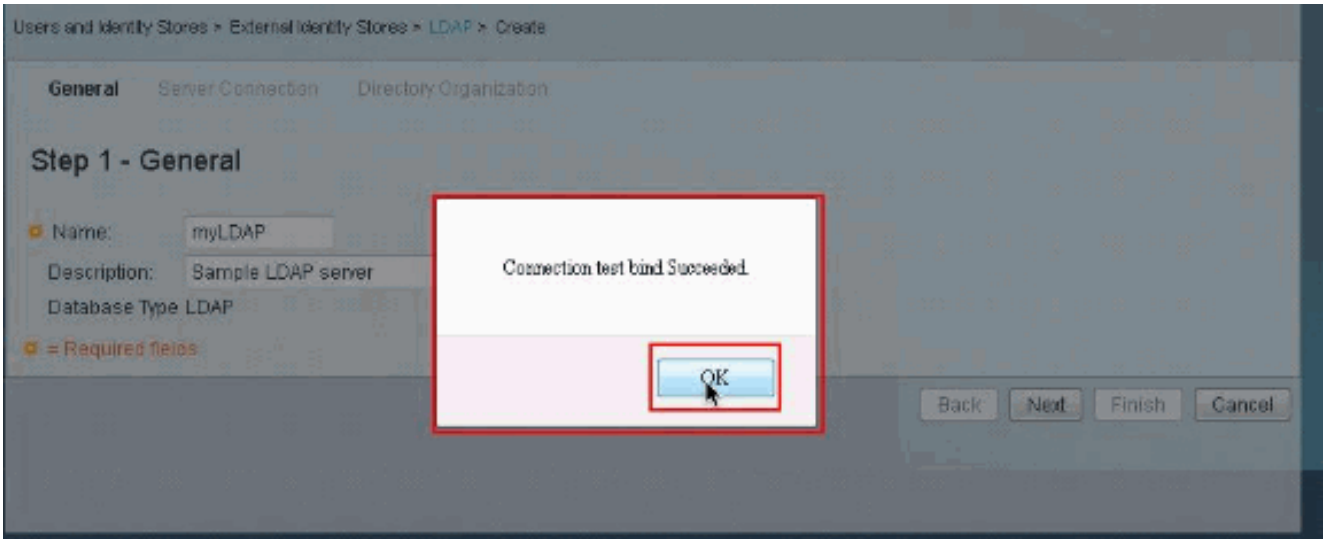
2. От **Вкладки Общие** предоставляют **Название** и **Описание** (дополнительное) для нового LDAP, затем нажимают
   Next.



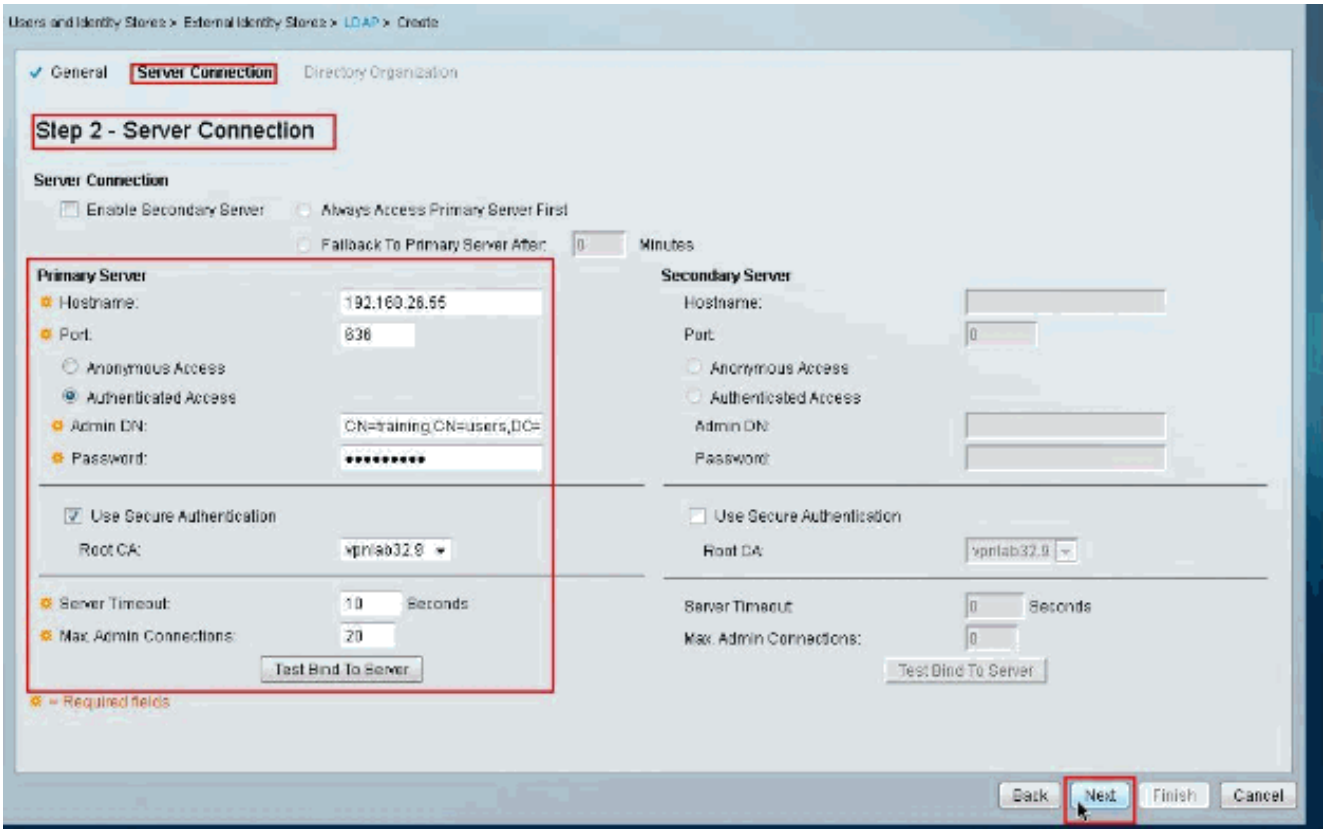
3. От вкладки **Server Connection** под разделом **Основного сервера** предоставьте **Имя хоста, порт, DN Admin и Пароль**. Гарантируйте, что флажок затем для **Использования Безопасной аутентификации** проверен, и выберите недавно установленный **Корневой сертификат CA**. Нажмите **Test Bind To Server**.**Примечание:** Номер назначенного порта IANA для безопасного LDAP является TCP 636. Однако подтвердите номер порта, который ваш Сервер LDAP использует от вашего Admin LDAP.**Примечание:** DN Admin и Пароль должны быть предоставлены вам вашим Admin LDAP. DN Admin, должно быть, считал все разрешения на всех OU на Сервере
LDAP.



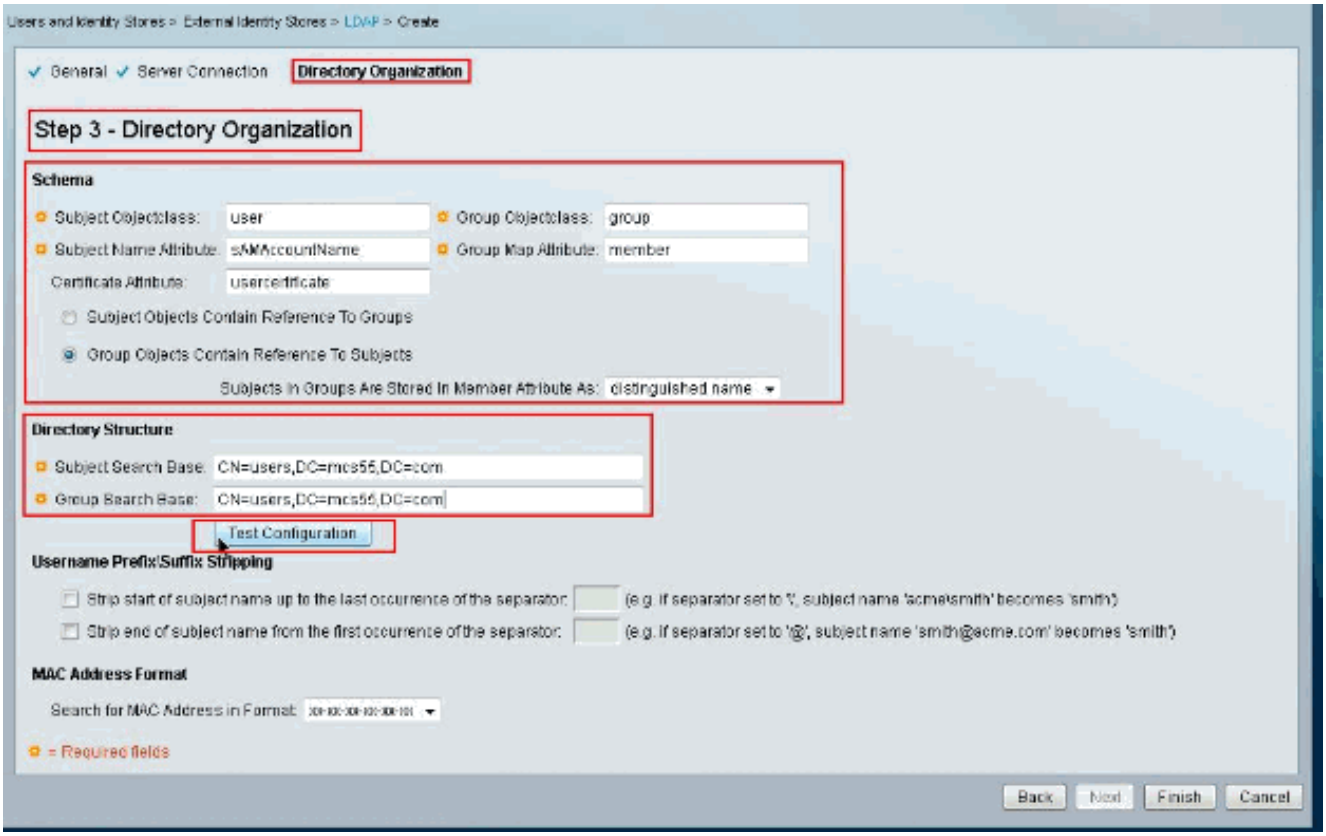
Следующий образ показывает, что **Тест соединения Связывает с сервером**, было успешно.**Примечание:** Если Тест Связывает, не успешно, тогда повторно проверяют **Имя хоста, Номер порта, DN Admin, Пароль** и **Узел CA** от вашего Администратора LDAP.



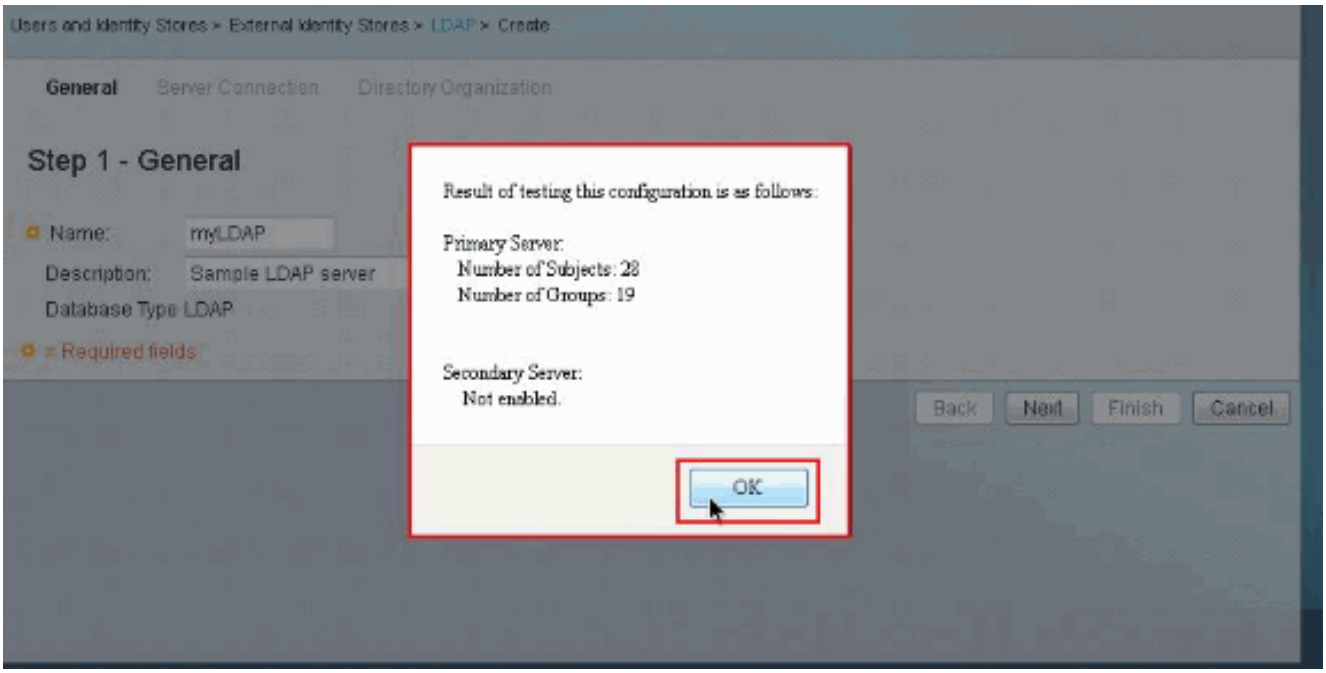
4. Нажмите кнопку **Next.**



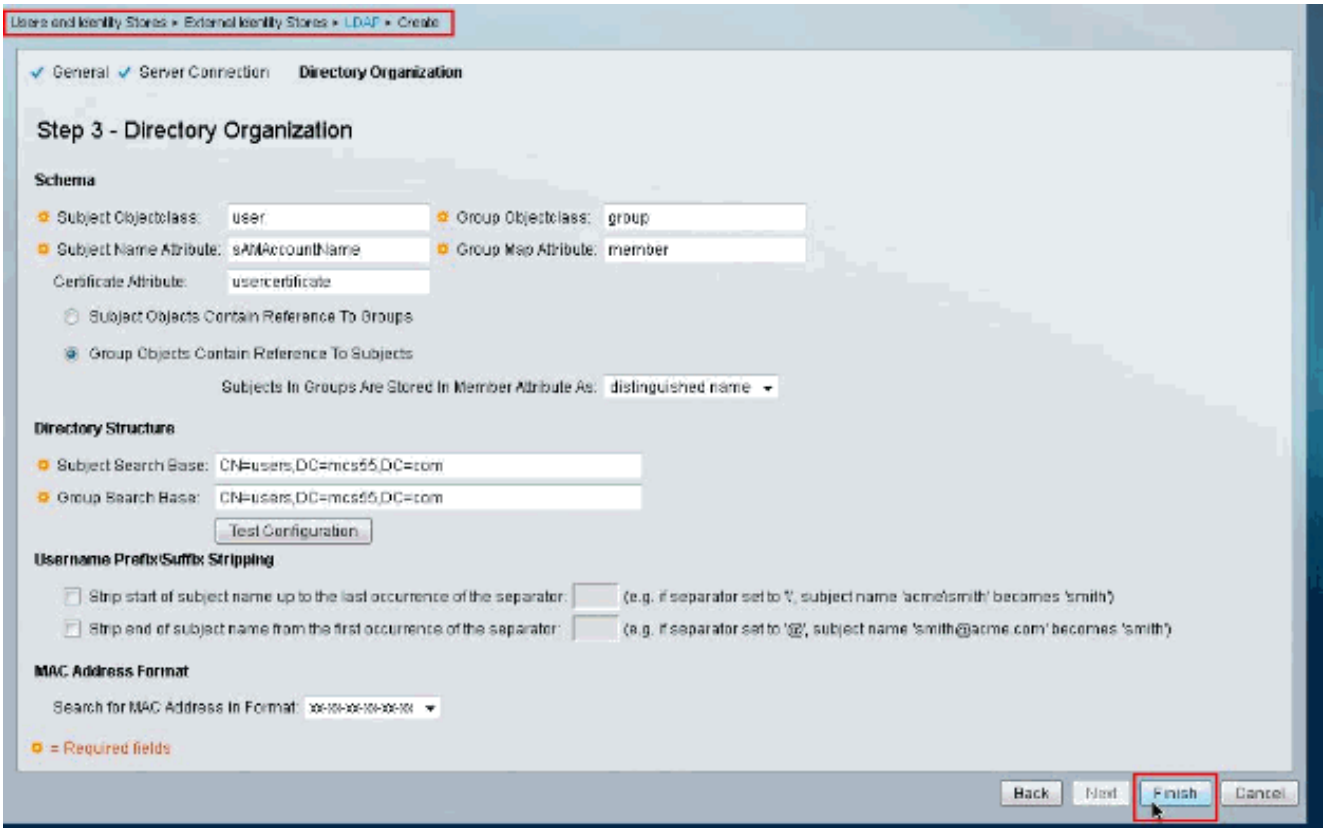
5. От вкладки **Directory Organization** под разделом **Схемы** предоставьте требуемую подробную информацию. Точно так же предоставьте необходимую информацию под разделом **Структуры каталогов** в соответствии с вашим Admin LDAP. Нажмите **Test Configuration**.



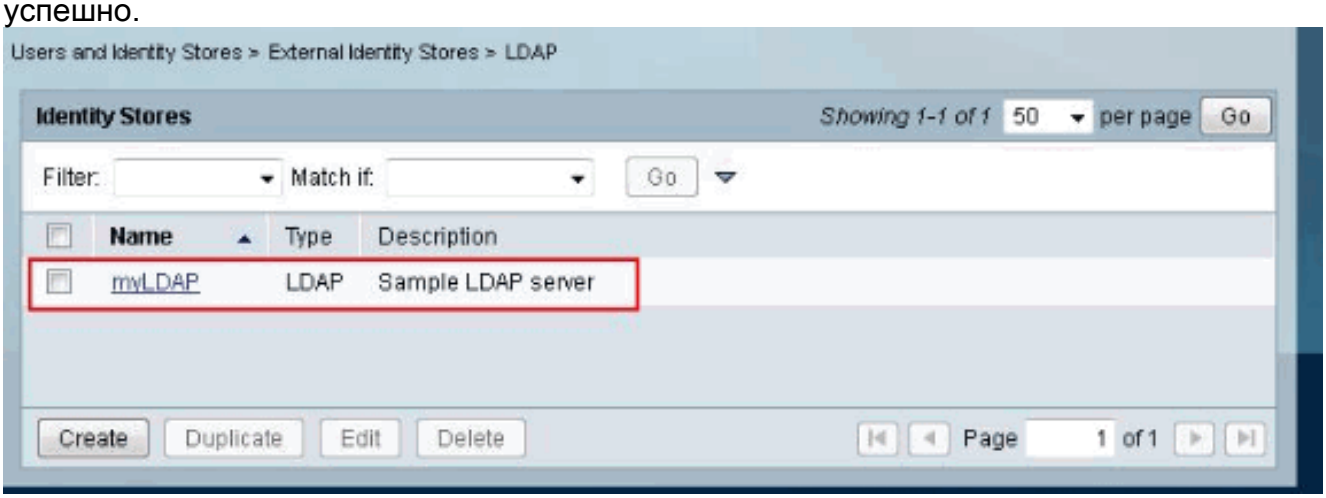
Следующий образ показывает, что **Конфигурационное испытание** успешно.**Примечание:** Если Конфигурационное испытание не успешно, тогда повторно проверяют параметры, предоставленные в **Схеме** и **Структуре каталогов** от вашего Администратора
LDAP.



6. **Нажмите кнопку**
   Finish.



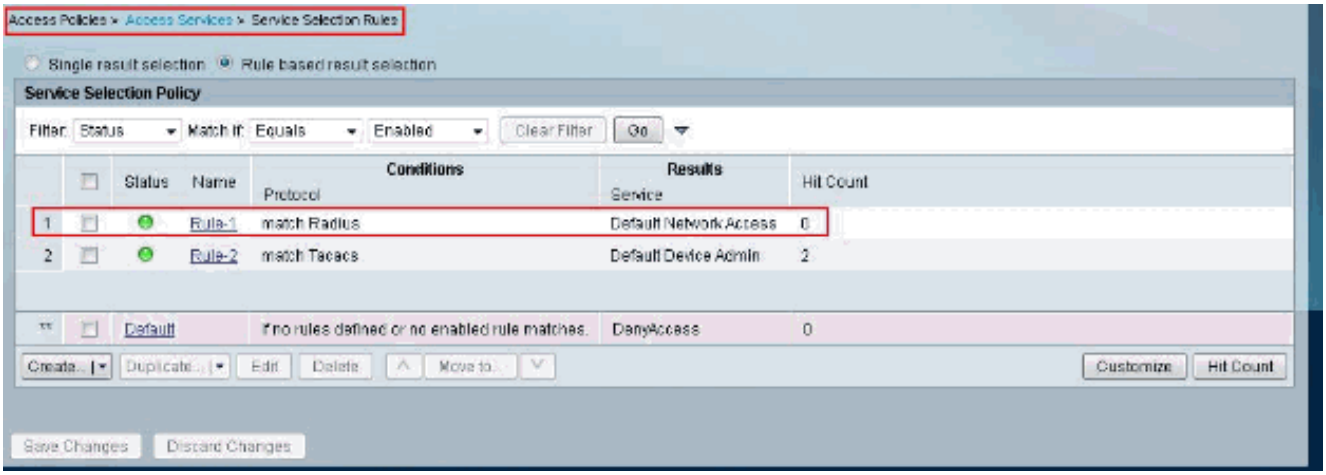
Сервер LDAP создан успешно.



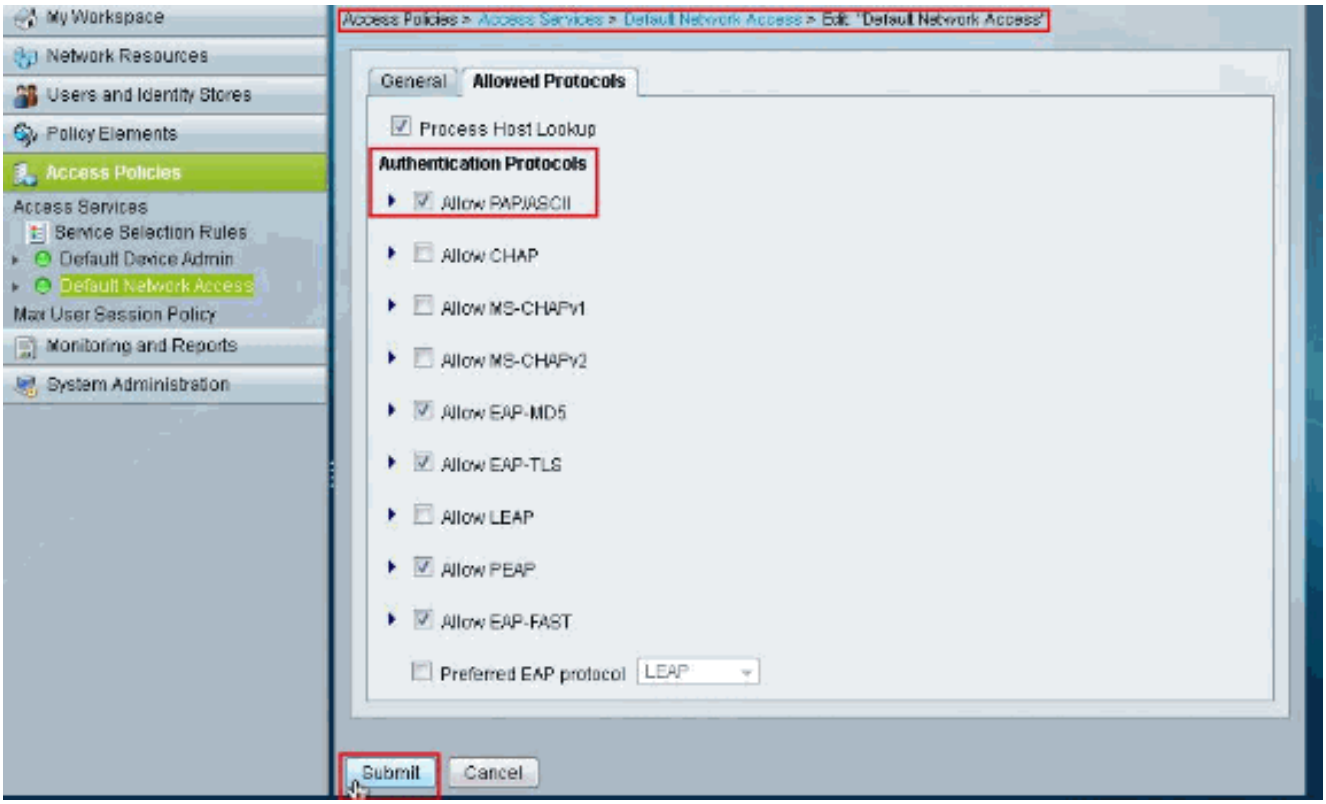
Настройте идентификационное хранилище

Конкурируйте эти шаги для настройки Идентификационного Хранилища:

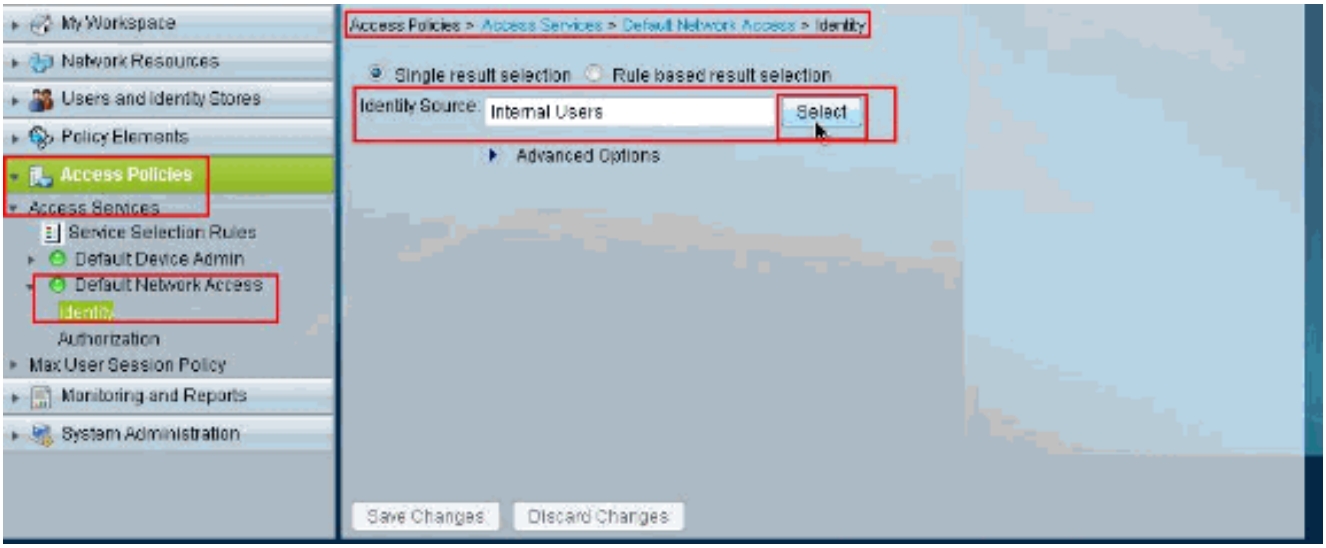
1. Выберите **Access Policies> Access Services> Service Selection Rules** и проверьте, какой сервис переходит к использованию Безопасный Сервер LDAP для Аутентификации. В данном примере сервисом является **Доступ к сети по умолчанию**.



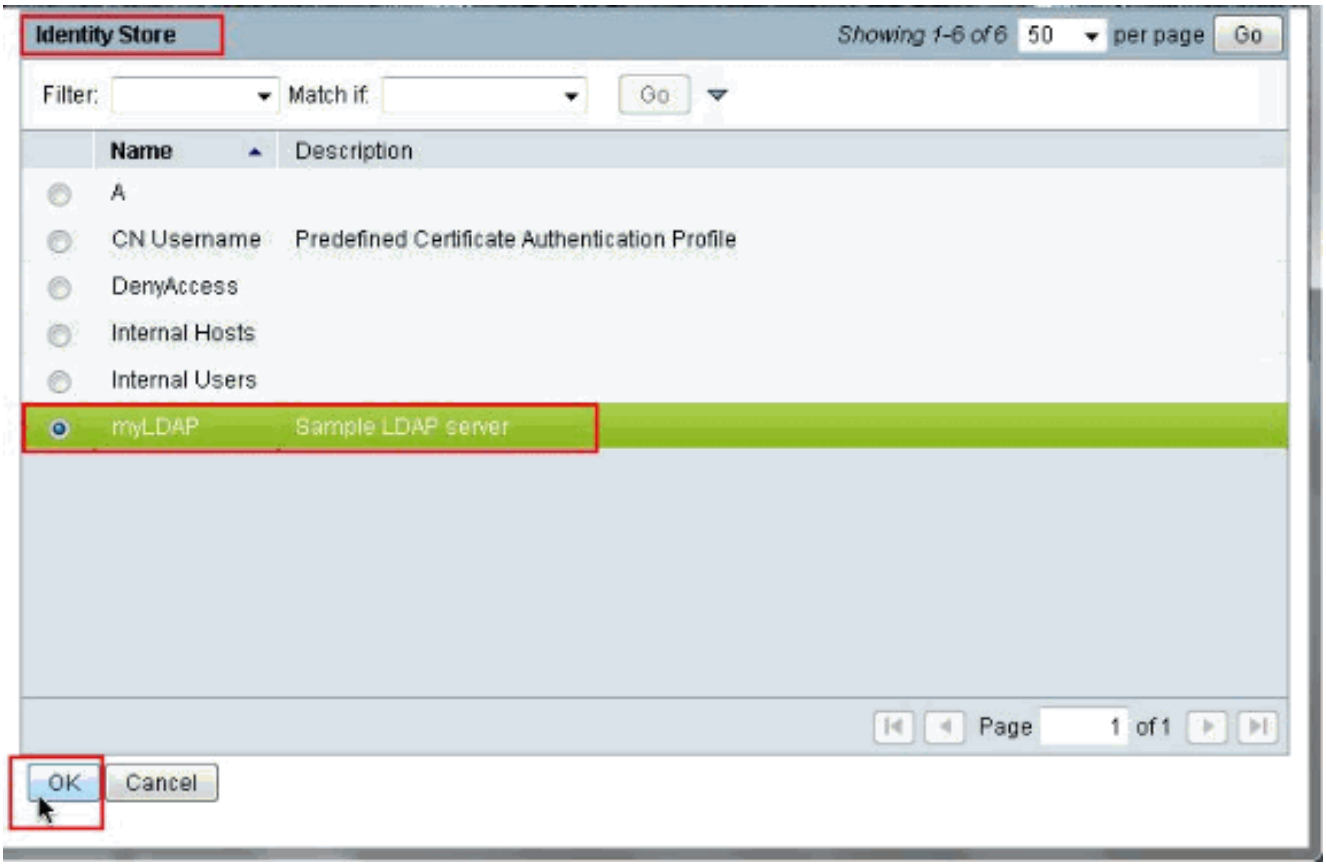
2. После того, как вы проверили сервис в шаге 1, переходите к определенному сервису и нажимаете **Allowed Protocols**. Гарантируйте, что **Позволяют, что PAP/ASCII** выбран, затем нажмите **Submit.Примечание:** Можно было выбрать другие протоколы аутентификации, Позволяют
PAP/ASCII.



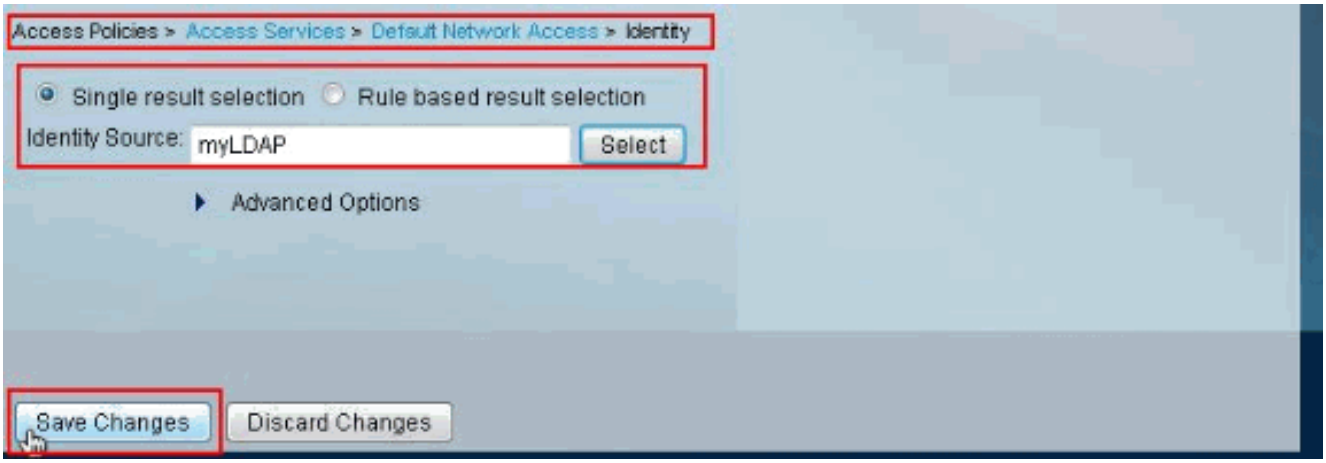
3. Нажмите сервис, определенный в шаге 1, затем нажмите **Identity**. Нажмите **Select**, следующий за **Идентификационным Источником**.



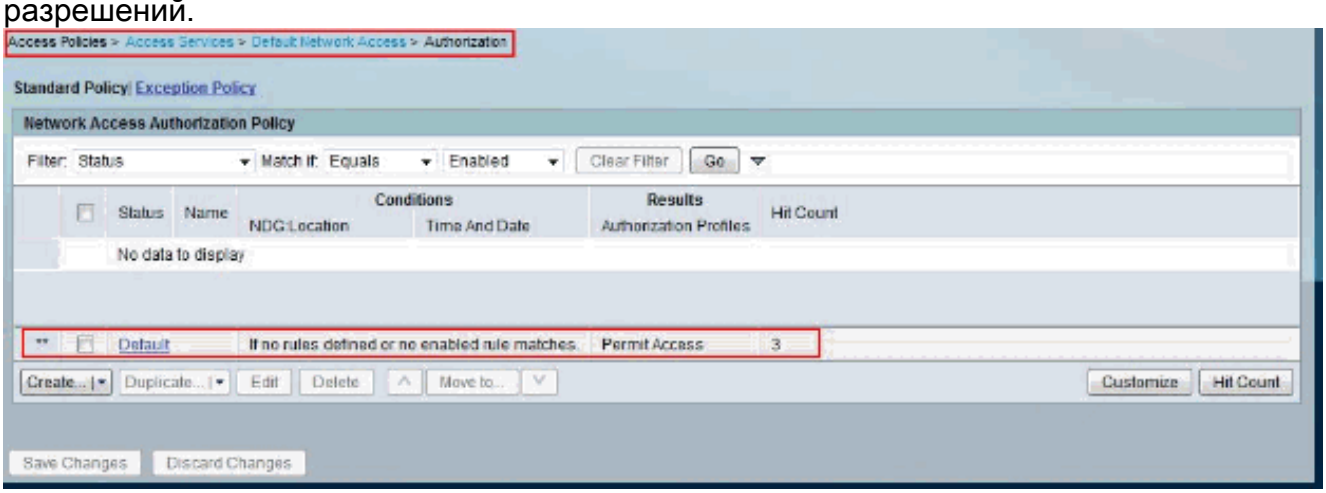
4. Выберите недавно созданный **безопасный Сервер LDAP** (**myLDAP** в данном примере), затем нажмите **OK**.



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



6. Перейдите к разделу **Авторизации** сервиса, определенного в **шаге 1**, и гарантируйте, 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, который указывает на возможную проблему с Сервером LDAP:

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

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

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

Дополнительные сведения

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