

Когда Active Directory облегченного доступа к каталогам (AD LDS) работает на компьютере, подключенном к домену, то экземпляр AD LDS пытается создать serviceConnectionPoint (SCP) объекта в области так, чтобы другие компьютеры в домене могли определить местонахождение LDS AD экземпляра.

В качестве опции, администратор может указать контейнер для создания этого объекта.

Контейнер должен существовать в домене прежде чем он сможет быть использован в качестве SCP.

Настройка доступа или отключение создания SCP

У вас есть два варианта:

1. Если вы не хотите, чтобы другие компьютеры в домене, чтобы иметь возможность определить местонахождение Directory облегченного служб Active (AD LDS) экземпляры, вы можете отключить создание serviceConnectionPoint (SCP) объектов в домене.
2. Если вы хотите, чтобы другие компьютеры имели возможность найти экземпляр AD LDS, убедитесь, что тип учетной записи службы является правильным и что он имеет соответствующие разрешения для создания SCP.

Выполните следующие процедуры с помощью компьютера членов домена, который имеет доменные средства администрирования.

Для выполнения этих процедур, необходимо иметь членство в **группе Администраторы домена** или вам должны быть делегированы соответствующие полномочия.

Отключение Создание SCP

Чтобы отключить создание SCP для всех экземпляров AD LDS, в наборе конфигурации:

1. Откройте редактор ADSI. Чтобы открыть ADSI Edit, нажмите **кнопку Пуск**, в поле **Начать поиск**

введите

adsiedit.msc

, и нажмите клавишу ВВОД.

Если

контроль учетных записей

Появится диалоговое окно, убедитесь, что в нем действия, что вы хотите, и нажмите кнопку

Продолжить

2. В дереве консоли щелкните правой кнопкой мыши объект ADSI Edit, а затем нажмите **Подключиться к**.

3. Убедитесь, что **Выберите известный контекст именования** выбран и что опция установлена в **конфигурации**

4. Убедитесь, что **Выберите или введите домен или сервер** выбран, а затем введите имя сервера следует двоеточие и сетевой порт на котором выполняется служба AD LDS доступен, например, **server1: 389**

Если вы работаете локально на сервере, на котором размещен экземпляр AD LDS, можно ввести

локальный: 389

, при условии, что экземпляр AD LDS предлагается через порт 389.

5. Перейдите к следующей папке под контейнере конфигурации: **CN = Configuration, CN = GUID CN = Services CN = Windows NT CN = Directory Service CN = SCP Публикация служба**, где **GUID**

является глобальным уникальным идентификатором (GUID) для AD LDS экземпляра.

Примечание: Объекты в ADSI Edit открываются в обратном порядке, в котором они записаны в облегченный протокол доступа к каталогам формате (LDAP).

например, если путь

CN = Сервер1, CN = Computers, DC = Contoso, DC = COM

в тексте событий, расширить
DC = Contoso, DC = COM
объект сначала, рядом
расширить CN = Computers
, а затем выберите
CN = Server1

6. Щелкните правой кнопкой мыши **Публикация Service CN = SCP** запись, а затем найдите атрибут **Enabled**

7. Дважды щелкните **Enabled** значение, выберите **значение False** , а затем нажмите **ОК** дважды.

Настройка разрешений для разрешения создания SCP

Чтобы убедиться, что тип учетной записи службы является правильным:

1. Откройте Службы. Для открытия меню Услуги, нажмите **кнопку Пуск** , в поле **Начать поиск** введите **services.msc** и нажмите клавишу ВВОД. Если **контроль учетных записей** Появится диалоговое окно, убедитесь, что в нем действия, что вы хотите, и нажмите кнопку **Продолжить**

2. Найдите AD LDS имя экземпляра в списке служб щелкните правой кнопкой мыши его, а затем нажмите **Свойства** .

3. Выберите **Вход в систему** и убедитесь, что **локальная системная учетная запись** не выбран.

Если он выбран, нажмите

учетной записью

, а затем введите

Network Service

или имя учетной записи пользователя домена, который вы хотите экземпляр AD LDS в использовании:

- Если вы используете Network Service, снимите **пароль** и **Подтверждение пароля**.
- Если вы используете учетную запись пользователя домена, введите и подтвердите пароль для этой учетной записи.
- Нажмите **ОК** для подтверждения изменений в учетной записи службы.

- Нажмите **ОК**, если вам будет предложено подтвердить, что счет должен быть предоставлено право на вход в качестве службы и что перезапуск сервиса не требуется.

- Не закрывайте оснастку Службы, потому что вы будете использовать его, чтобы перезапустить экземпляр AD LDS в конце этих процедур.

Чтобы подтвердить, что учетная запись службы имеет соответствующие разрешения:

1. Откройте редактор ADSI. Чтобы открыть ADSI Edit, нажмите **кнопку Пуск**, в **поле Начать поиск**

введите

adsiedit.msc

, и нажмите клавишу ВВОД.

Если

контроль учетных записей

Появится диалоговое окно, убедитесь, что в нем действия, что вы хотите, и нажмите кнопку

Продолжить

.

2. В дереве консоли щелкните правой кнопкой мыши объект ADSI Edit, а затем нажмите **Подключиться к**.

3. Убедитесь, что **Выберите известный контекст именован** выбран и что опция установлена в **умол**

чанию контекст именован

.

4. Убедитесь, что **Выберите или введите домен или сервер** выбран, а затем введите имя контроллера домена, за которым следует номер порта, на котором

доменных служб Active Directory (AD DS) размещен (по умолчанию, 389).
Например, чтобы подключиться к контроллеру домена с именем ContosoDC1 на порт 389, типа

ContosoDC1: 389

Характерное имя SCP идентифицируется в тексте событий Просмотр событий.

5. Найдите родительский объект идентифицированного SCP (родительский объект SCP):

- По умолчанию родительский объект является учетная запись компьютера компьютере, где размещен экземпляр AD LDS.

- Чтобы определить имя родительского объекта, использовать путь из текста событий, без CN = { *GUID* } части (которая является именем SCP, который должен был быть создан).

- Вы также должны расширить объекты в ADSI Edit в обратном порядке, в котором они появляются в тексте событий. Например, если путь **CN = *GUID* }, CN =**

Сервер1, CN = Computers, DC = Contoso, DC = COM

в тексте событий, разверните объект

DC = Contoso, DC = COM

во-первых, расширить

CN = Computers

, а затем выберите

SERVER1

объект, потому что он является родителем расположение ПКПП.

- Щелкните правой кнопкой мыши родительский объект SCP, а затем нажмите **Свойства**.

- Нажмите **Security**.

- Нажмите **Добавить**, чтобы добавить пользователя домена или учетную запись группы. Убедитесь, что учетная запись, назначить в качестве

учетной записи службы имеет

объектов

всех дочерних объектов

разрешения, установленные на

Разрешить

Создать всех дочерних и Удаление

- Чтобы подтвердить эти изменения, нажмите **ОК**.

- Вернуться к оснастке Службы, а затем перезапустить экземпляр AD LDS. Чтобы перезапустить экземпляр AD LDS, щелкните правой кнопкой мыши имя экземпляра и нажмите кнопку

Перезагрузка

Проверка

Когда Active Directory облегченного доступа к каталогам (AD LDS) экземпляр успешно создает serviceConnectionPoint (SCP), Код события 2535 регистрируется в журнале событий. Проверьте наличие этого события в ADAM_ *INSTANCENAME* журнале просмотра событий, где *имя_экземпляра* это имя экземпляра AD LDS.

Источник: technet.microsoft.com