

Администрирование Windows Server 2012

Лабораторная работа № 3. Делегирование и безопасность объектов Active Directory

На этом занятии мы обсудим, как делегировать конкретные административные задачи в Active Directory путем изменения списков контроля доступа ACL (Access Control List) для объектов Active Directory.

Упражнение 1. Делегирование управления и поддержки учетных записей пользователей

В этом упражнении вы разрешите группе Справка сбрасывать пароли пользователей и снимать блокировку учетных записей в подразделении Кадры.

1. Войдите на машину SERVER01 как администратор и откройте оснастку Active Directory — пользователи и компьютеры.
2. Разверните узел домена contoso.com, щелкните правой кнопкой мыши подразделение Кадры и примените команду Делегирование управления, запуская Мастер делегирования управления.
3. Щелкните кнопку Далее.
4. На странице Пользователи или группы щелкните кнопку Добавить.
5. В диалоговом окне Выбор введите имя Справка и щелкните ОК.
6. Щелкните кнопку Далее.
7. На странице Делегируемые задачи выберите задачу Переустановить пароли пользователей и установить изменение пароля при следующей перезагрузке.
8. Щелкните кнопку Далее (Next).
9. Просмотрите выбранные действия и щелкните кнопку Готово.

Упражнение 2. Просмотр делегированных разрешений

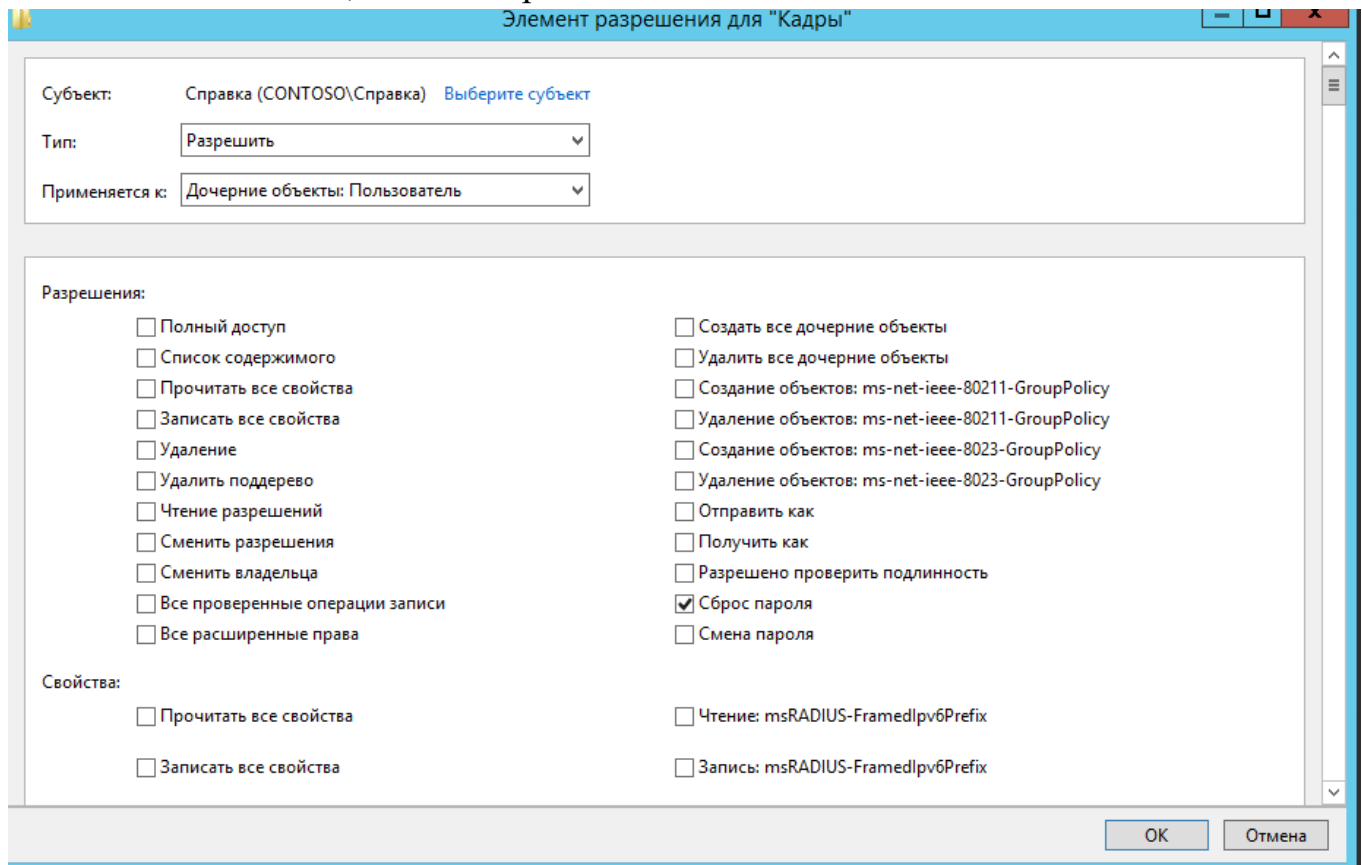
В этом упражнении вы просмотрите разрешения, назначенные для подразделения Справка.

1. Войдите на машину SERVER01 как администратор и откройте оснастку Active Directory — пользователи и компьютеры.
2. Щелкните правой кнопкой мыши подразделение Кадры и примените команду Свойства. Вкладка Безопасность не будет отображаться, если не включены Дополнительные компоненты.
3. Щелкните ОК, чтобы закрыть диалоговое окно Свойства.
4. Щелкните меню Вид и установите флажок Дополнительные компоненты.
5. Щелкните правой кнопкой мыши подразделение Кадры и примените команду Свойства (Properties).
6. Перейдите на вкладку Безопасность.
7. Щелкните кнопку Дополнительно.

8. В списке Элементы разрешений выберите первое разрешение, назначенное подразделению Справка.

9. Щелкните кнопку Изменить (Edit).

10. В диалоговом окне Элемент разрешения отыщите назначенное разрешение, а затем щелкните ОК, чтобы закрыть диалоговое окно.



11. Повторите шаги 8-10, чтобы просмотреть второе разрешение подразделения Справка.

12. Повторите шаги 2-11, чтобы просмотреть список ACL пользователя в подразделении Кадры и проанализировать унаследованные разрешения, назначенные подразделению Справка.

13. Откройте окно командной строки, введите dscls "ou=Кадры,dc=contoso,dc=com"и нажмите клавишу Enter.

14. Просмотрите разрешения, назначенные подразделению Справка.

Упражнение 3. Проверка делегированных прав и анализ наследования

В этом задании вы проверите успех делегирования и выясните, что произойдет, если администратор попытается выполнить задание, которое не было ему делегировано. Вы также проанализируете результаты наследования и защиту подразделения.

- Подразделение Администраторы должно содержать учетную запись пользователя и группу Справка.
- Должна быть учетная запись для Барбары Майер и хотя бы одна учетная запись в подразделении Кадры.

- Пользователю Барбаре Майер следует быть членом группы Справка.
- Группе Справка должны быть делегированы разрешения Переустановить пароли пользователей и установить изменение пароля при следующей перезагрузке для подразделения Кадры.

1. Войдите на SERVER01 как пользователь Барбара Майер (bmayer) с её паролем.

2. Откройте оснастку Active Directory — пользователи и компьютеры.

3. Разверните домен contoso.com и перейдите в подразделение Кадры.

4. Щёлкните правой кнопкой мыши по любому пользователю в этом подразделении (например, user1) и выберите Сбросить пароль.

5. Введите новый пароль (например, P@ssword123) и снимите флажок «Требовать смену пароля при следующем входе». Нажмите ОК.

6. Пароль успешно изменён, ошибок нет. Это подтверждает, что делегированное право работает.

7. Оставаясь в оснастке ADUC под учётной записью Барбары, попробуйте создать нового пользователя в подразделении Кадры: Щёлкните правой кнопкой по подразделению Кадры → Создать → Пользователь.

8. Заполните любые поля и попытайтесь завершить создание.

9. Появится сообщение об ошибке «Недостаточно прав» или «Отказано в доступе». Это правильно, так как создание объектов не было делегировано группе «Справка».

10. Попробуйте удалить любого пользователя в подразделении Кадры (через правую кнопку → Удалить). Аналогичная ошибка — удаление запрещено.