

Администрирование Windows Server 2012

Лабораторная работа № 5. Группы пользователей

На любом предприятии пользователи, компьютеры и даже службы со временем меняются, бизнес-роли и правила обычно более стабильны. Поэтому основные права и разрешения отдельным пользователям, компьютерам или объектам идентификации служб напрямую не назначают. Задачи, связанные с управлением, должны быть привязаны к группам.

Группа - это совокупность учетных записей, компьютеров и вложенных групп, упрощающая задачу администрирования.

Типы групп:

Группы распространения	Создаются для массовых рассылок информации пользователям, входящим в группу, не влияют на права. Не являются субъектами безопасности и не содержат SID-идентификаторы. Поэтому им нельзя назначать разрешения доступа к ресурсам. Сообщение, отправленное группе распространения, будет переслано всем ее членам.
Группы безопасности	Можно использовать как элемент разрешения, управления доступа к ресурсу. Это принципы безопасности с SID-идентификаторами.

Область действия группы	Члены группы из того же домена	Члены группы из другого домена в том же лесу	Члены группы из доверенного внешнего домена
Локальная	Пользователи, компьютеры, глобальные группы, универсальные группы, локальные группы в домене, локальные пользователи, определенные на том же компьютере, где определена локальная группа	Пользователи, компьютеры, глобальные группы и универсальные группы	Пользователи, компьютеры, глобальные группы
Локальная в домене	Пользователи, компьютеры, глобальные группы, универсальные группы, локальные группы в домене	Пользователи, компьютеры, глобальные группы и универсальные группы	Пользователи, компьютеры, глобальные группы
Универсальная	Пользователи, компьютеры, глобальные группы и универсальные группы	Пользователи, компьютеры, глобальные группы и универсальные группы	Нет доступа
Глобальная	Пользователи, компьютеры, глобальные группы	Нет доступа	Нет доступа

Характеристики, определяющие каждую область действия группы, распределены по следующим категориям.

- **Репликация.** Где определена группа и на какие системы выполняется ее репликация.

- *Членство.* Какие типы принципалов безопасности группа может содержать в качестве членов. Может ли группа включать принципалы безопасности из доверенных доменов.

- *Доступность.* Где будет использоваться группа. Можно ли включить эту группу в другую группу. Можно ли добавить группу в список ACL.

Эти характеристики следует продумать при определении области действия каждой группы.

Группы содержат элементы, управляют группами как одним объектом. Реализация управления группами в Active Directory не так проста, поскольку структура Active Directory предназначена для поддержки крупных распределенных сред и включает семь типов групп: две группы домена с тремя областями действия в каждой и локальные группы безопасности.

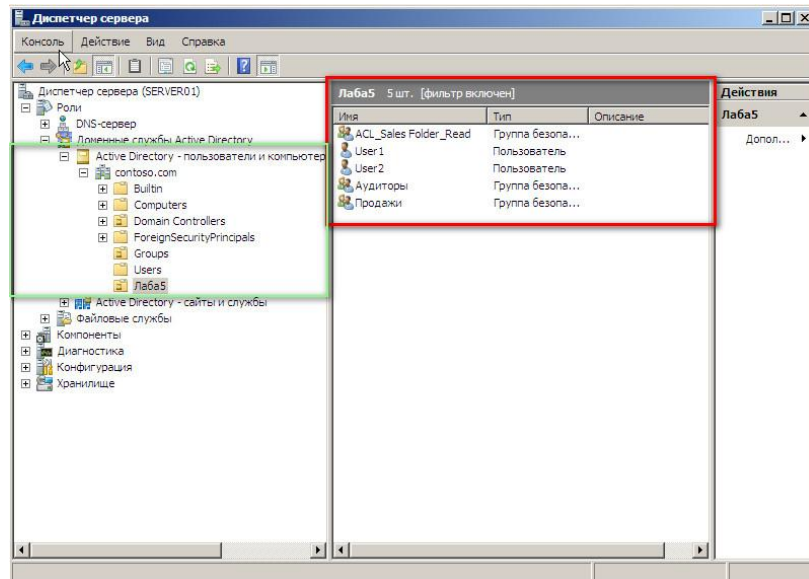
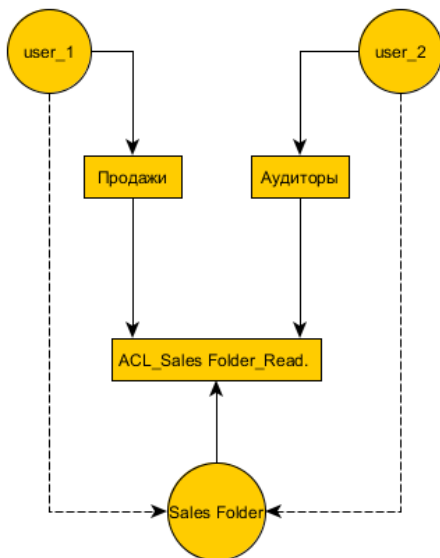
Группы представляют собой принципалы безопасности с идентификатором безопасности SID (Security Identifier), которые содержат в своем атрибуте member другие принципалы безопасности (пользователи, компьютеры, контакты и прочие группы), позволяя таким образом повысить эффективность управления.

Например, всем 100 пользователям в отделе продаж требуется доступ чтения к общей папке на сервере. Нет смысла назначать разрешения доступа каждому отдельному пользователю, поскольку при приеме на работу новых менеджеров по продажам в список контроля доступа ACL (Access Control List) папки придется добавлять новые учетные записи. При удалении учетных записей из списка ACL понадобится удалить разрешения доступа, иначе в ACL останется отсутствующая учетная запись, ведь SID-идентификатор в ACL ссылается на учетную запись, которую невозможно разрешить. Представим, что всем 100 пользователям в отделе продаж потребуется доступ к 10 общим папкам на трех серверах. Управление этими пользователями значительно усложнится.

Вместо разрешений доступа к ресурсу отдельным объектам идентификации (например, пользователям и компьютерам) рекомендуется назначить одно разрешение доступа группе, а затем управлять доступом к ресурсу, изменяя членство в этой группе.

1. Создание групп пользователей. Организация доступа к сетевому ресурсу через группу, предоставляющую права

Структура упражнения:

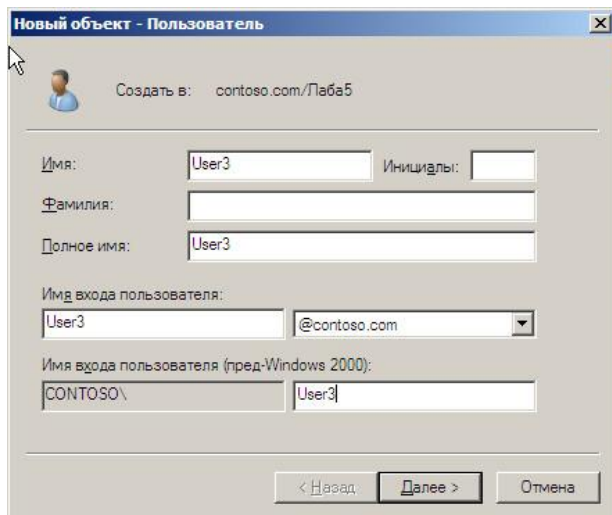


Упражнение 1. Создание пользователей с помощью шаблона пользовательской учетной записи

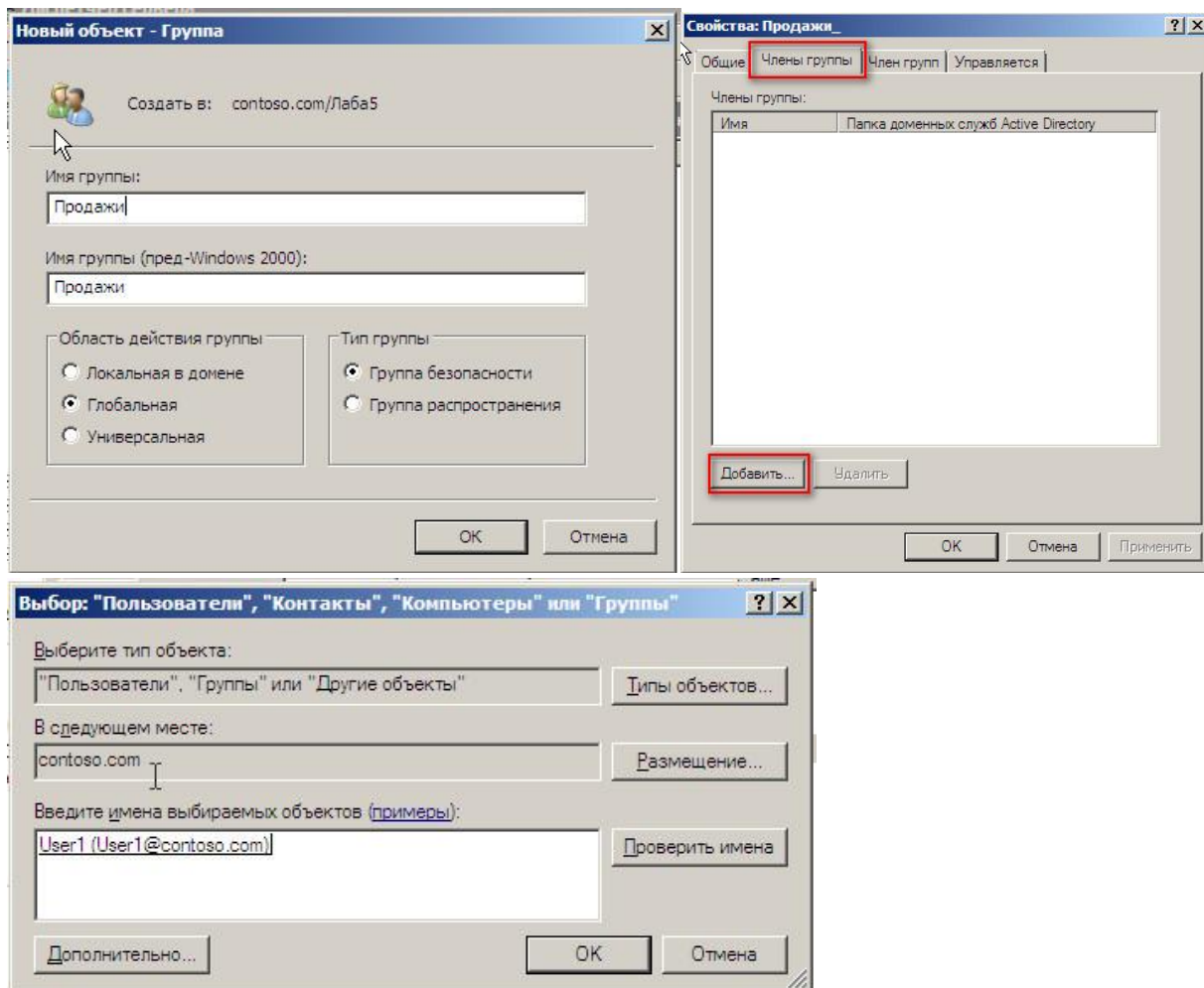
В этом упражнении вы создадите для менеджеров по продажам шаблон пользовательской учетной записи, предварительно заполненный свойствами. Затем вы создадите учетную запись пользователя для нового менеджера по продажам, скопировав шаблон пользовательской учетной записи.

1. Войдите на машину SERVER01 как администратор и создайте подразделение Лаба5.

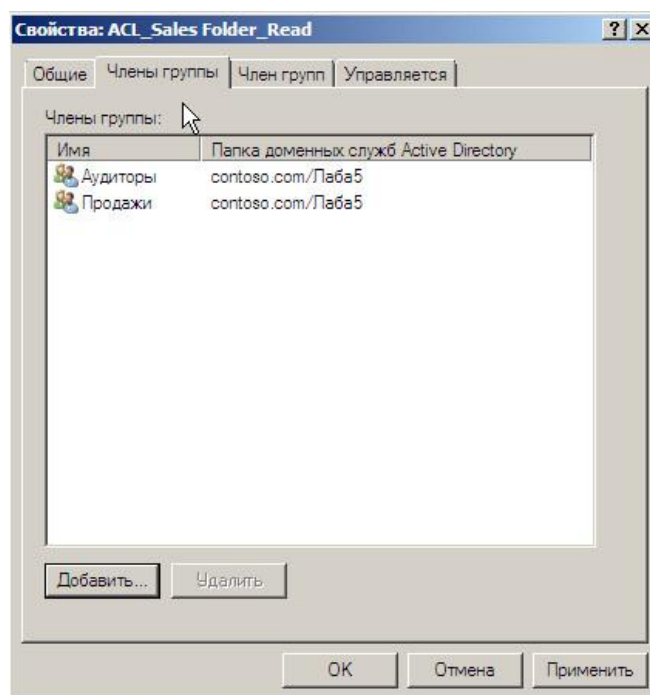
2. Создайте пользователей User1, User2.



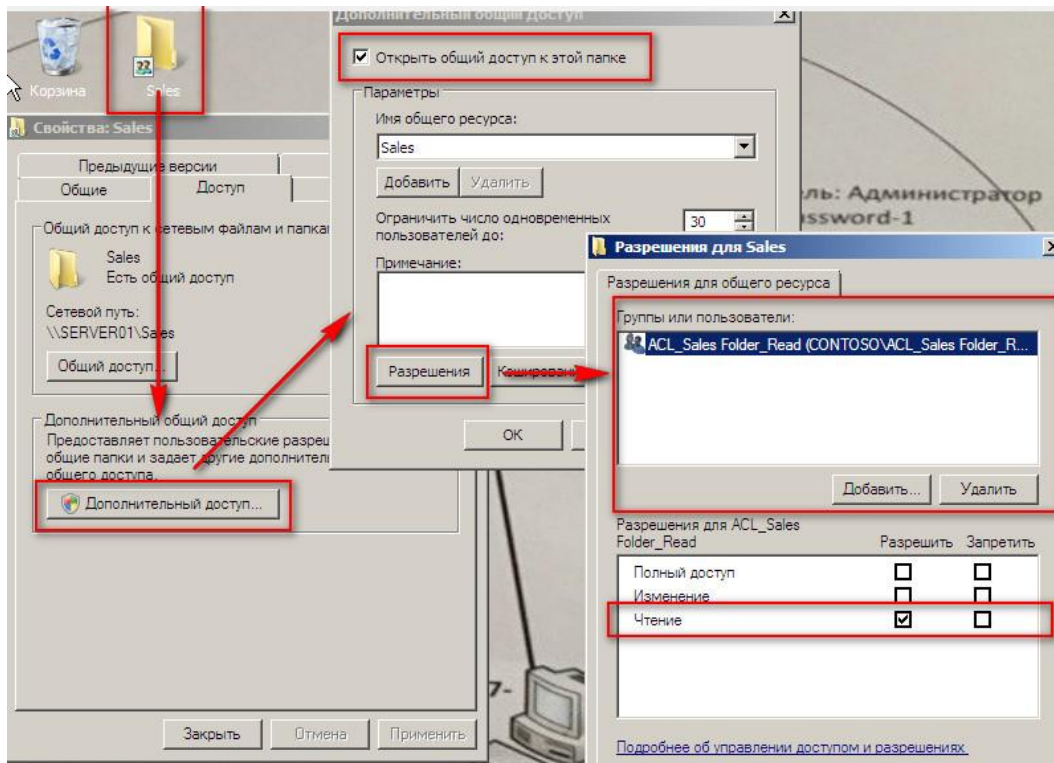
3. Создайте глобальные группы Продажи_, Аудиторы. Включите пользователя User1 в группу Продажи, пользователя User2 в группу Аудиторы.



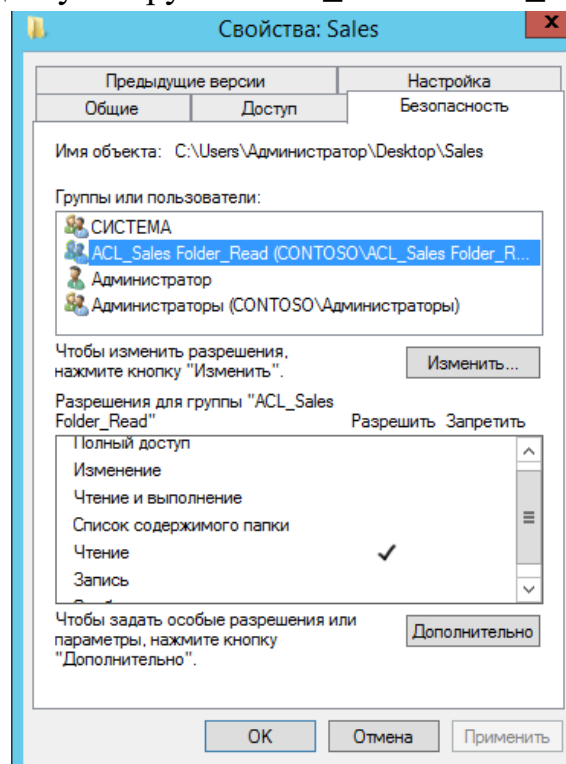
4. Создайте локальную группу в домене ACL_Sales Folder_Read (мы создадим группу, которая будет иметь доступ к сетевой папке Sales спецификация имени группы: access list_<имя папки>_<Права>) Добавьте в эту группу группы Продажи и Аудиторы.



5. Создайте папку Sales, в ней текстовый файл. Включите удаленный доступ к папке, задайте параметры доступа: группа ACL_Sales Folder_Read только для чтения.



6. Перейдите на вкладку Безопасность (Security). Щелкните кнопку Изменить (Edit), а затем щелкните кнопку Добавить (Add). Включите удаленный доступ к папке, задайте параметры доступа: группа ACL_Sales Folder_Read только для чтения.

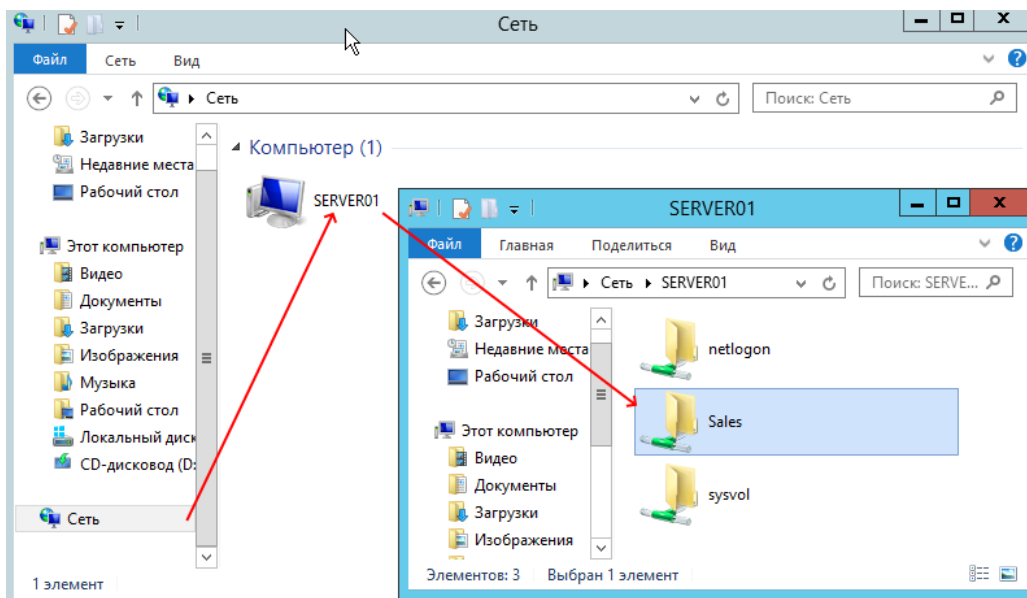


7. Если сетевое окружение отключено, то включить его.

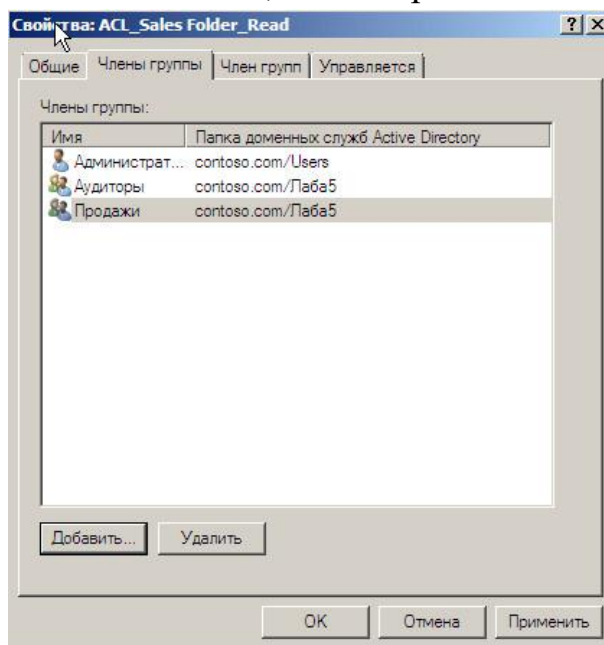
запустите службы, от которых зависит сетевое обнаружение:

1. Нажмите Win + R, введите services.msc и нажмите Enter.
2. В списке служб найдите Публикация ресурсов обнаружения функции и запустите ее:

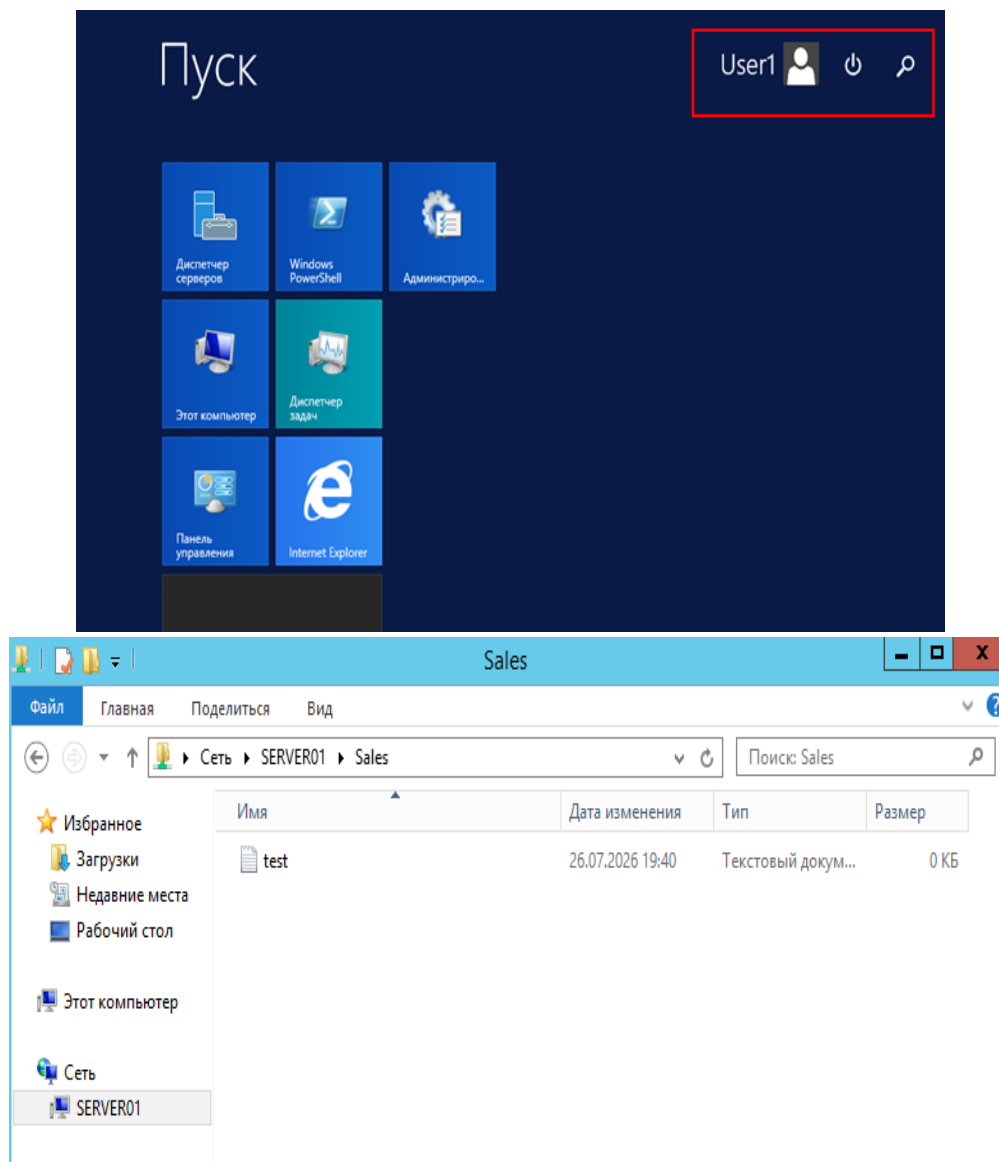
7. Попробуйте зайти в папку Sales через сетевое окружение.



8. Добавьте пользователя Администраторы в группу ACL_Sales Folder_Read. Перезайдите (выполнив выход из системы, чтобы применились изменения групп).



9. При наличии других компьютеров в домене произведите авторизацию от пользователя, находящегося в группе ACL_Sales Folder_Read (User1 или User2), и получите доступ к папке Server01\Sales.



2. Установка компьютера в домене

Дэн Холме: «Компьютеры тоже люди» — по крайней мере, так они воспринимаются в Active Directory. Компьютеры имеют атрибут objectclass пользователя. Как и пользователи, компьютеры имеют учетные записи.

- Если объект существует и компьютер с таким именем уже присоединен к домену, возникнет ошибка и вы не сможете присоединить компьютер к домену.
- Если объект существует и предварительно размещен (компьютер с таким же именем, не присоединенный к домену), домен подтверждает, что введенная учетная запись имеет разрешение на присоединение компьютера к домену.
- Если учетная запись компьютера не была предварительно размещена, Windows проверяет, имеете ли вы разрешение на создание нового объекта компьютера в контейнере компьютеров по умолчанию. Если вы располагаете разрешениями на создание нового объекта компьютера в контейнере по умолчанию, будет создан объект с именем компьютера. Этот метод присоединения к домену

поддерживается для обратной совместимости, но использовать его не стоит. Рекомендуется предварительно разместить учетную запись.

Как в любой ОС семейства Windows компьютер принадлежит к рабочей группе. Перед входом на компьютер с помощью доменной учетной записи нужно присоединить компьютер к домену. Для присоединения к домену компьютер должен располагать учетной записью в домене, которая, аналогично пользовательской учетной записи, содержит имя входа (атрибут sAMAccountName), пароль и идентификатор безопасности (SID), который уникальным образом представляет компьютер в домене как принципал безопасности. Эти учетные данные позволяют компьютеру проходить проверку подлинности в домене и создать безопасную связь, с помощью которой пользователи затем смогут войти в систему с применением учетных записей домена.

В рабочей группе каждая система поддерживает хранилище учетных записей пользователей и групп. Локальное хранилище объектов идентификации на каждом компьютере называется базой данных диспетчера безопасности учетных записей SAM (Security Accounts Manager). Если пользователь входит на компьютер рабочей группы, система выполняет проверку подлинности этого пользователя в своей локальной базе данных SAM. Если пользователь подключается к еще одной системе, например для получения доступа к файлу, вновь выполняется проверка подлинности пользователя в хранилище объектов идентификации удаленной системы. В отношении безопасности компьютер рабочей группы по всем параметрам — независимая автономная система.

Компьютер, присоединяемый к домену, делегирует ему задачу проверки подлинности пользователей. Хотя компьютер продолжает поддерживать свою базу данных SAM учетных записей локальных пользователей и групп, учетные записи пользователей, как правило, будут создаваться в центральном каталоге домена. Пользователь, входящий на компьютер посредством доменной учетной записи, теперь проходит проверку подлинности на контроллере домена, а не в базе данных SAM. Другими словами, компьютер доверяет контроллеру домена идентификацию пользователя. Доверительные отношения обычно рассматриваются в контексте двух доменов, однако доверие устанавливается также между каждым рядовым компьютером и его доменом; это происходит при присоединении компьютера к домену.

Для присоединения к домену Active Directory компьютер должен соответствовать трем требованиям:

- В службе каталогов должен быть создан объект компьютера.
- Вы должны иметь соответствующие разрешения доступа к объекту компьютера, включая право присоединения к домену компьютера с тем же именем, что у объекта в домене.

- Чтобы изменить членство компьютера в домене или рабочей группе, нужно быть членом локальной группы Администраторы (Administrators).

Контейнер Computers

Перед созданием объекта компьютера в службе каталогов (первое из трех требований для присоединения компьютера к домену) нужно определиться с контейнером, в который будет помещен этот объект. При создании домена по умолчанию создается контейнер Computers (CN=Computers,...). Этот контейнер — не подразделение, а именно объект класса container. Между контейнером и подразделением существует тонкое, но важное отличие. В контейнере нельзя создать подразделение (то есть не вы можете разбить контейнер Computers на подразделения), и к контейнеру нельзя привязать объект групповой политики.

Поэтому для управления компьютерами настоятельно рекомендуется создавать настраиваемые подразделения, а не использовать контейнер Computers.

Упражнение 1. Установка компьютера в домен contoso

Установка компьютера в домен contoso.com с предварительным созданием учетной записи компьютера в AD, и делегированием права добавления устройств в домен.

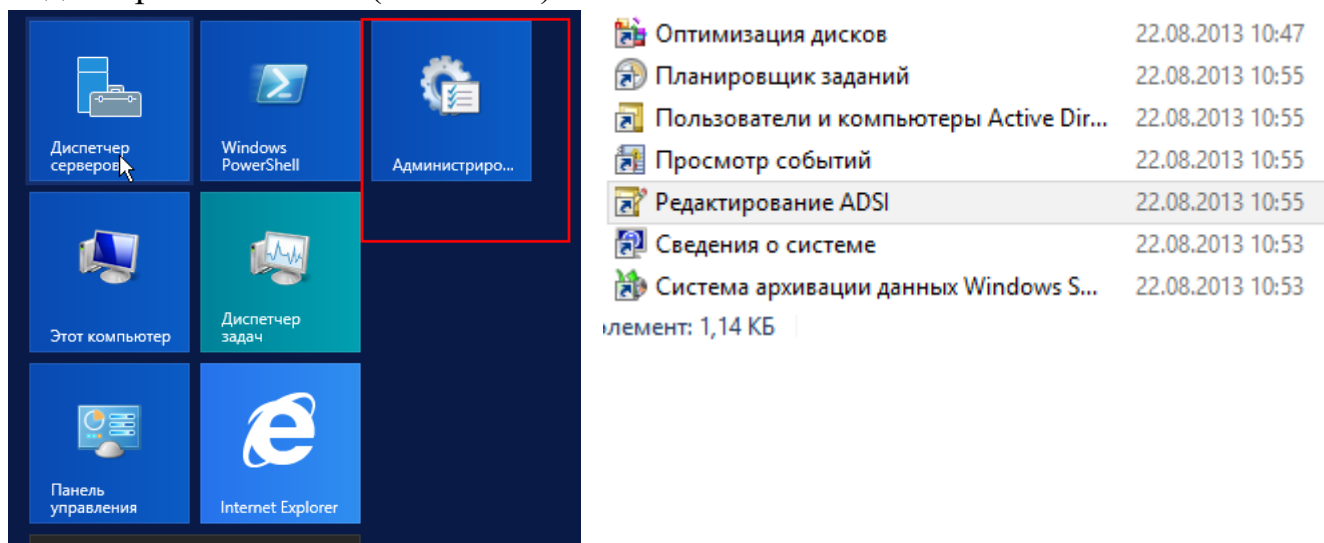
Для выполнения лабораторной работы необходимо 2 компьютера:

1 – контроллер домена, 2 – машина, которая будет добавляться в домен.

1. Войдите на машину SERVER01 как администратор.

2. Ограничение возможности создания компьютеров пользователями (безопасность):

2.1. В группе Администрирование (Administrative Tools) откройте оснастку Редактирование ADSI (ADSI Edit).



2.2. Щелкните правой кнопкой мыши узел Редактирование ADSI и примените команду Подключение к.

2.3. В секции Точка подключения выберите опцию Выберите известный контекст подключения, а в раскрывающемся списке выберите Контекст именования по умолчанию.

2.4. Щелкните ОК.

2.5. Разверните Контекст именования по умолчанию.

2.6. Щелкните правой кнопкой мыши, к примеру, папку домена dc=contoso,dc=com примените команду Свойства (Properties).

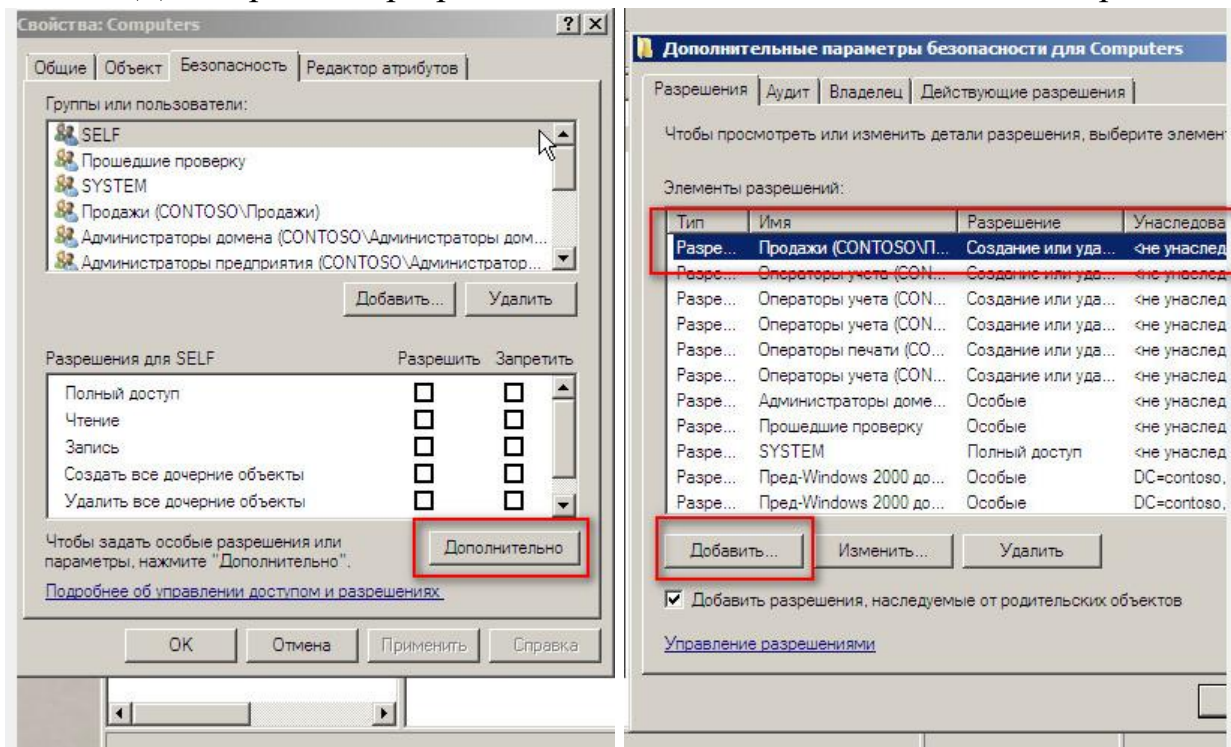
2.7. Выберите атрибут ms-DS-MachineAccountQuota и щелкните кнопку Изменить (Edit).

2.8. Введите значение 0.

2.9. Щелкните ОК.

3. Создайте группу, и пользователя в ней, который получит возможность добавлять компьютеры в домен (например, пользователя с именем test).

4. Делегирование разрешения на создание объектов Компьютеров



4.1. На машине SERVER01 откройте оснастку Active Directory — пользователи и компьютеры (Active Directory Users And Computers);

4.2. Щелкните меню Вид и установите флажок Дополнительные компоненты.

4.3. Щелкните правой кнопкой мыши на контейнер Computers и примените команду Свойства.

4.4. Перейдите на вкладку Безопасность.

4.5. Щелкните кнопку Дополнительно.

4.6. Щелкните кнопку Добавить.

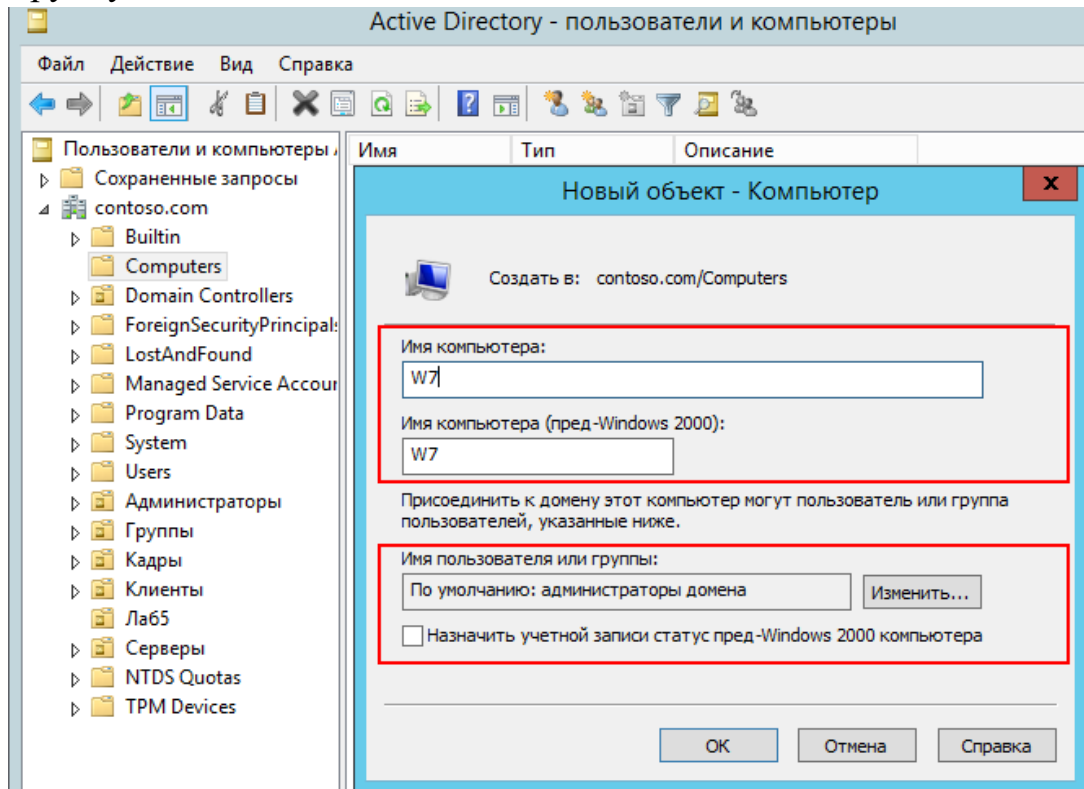
4.7. В разделе Субъект введите имя из п.3 test.

4.8. В списке «Применяется к» выберите уровень Этот объект и все дочерние объекты.

4.9. В списке Разрешения установите флажок Разрешить напротив Создание объектов: Компьютер (Create Computer Objects).

4.11. Трижды щелкните ОК, чтобы закрыть все диалоговые окна.

5. В контейнере Computers создайте запись для нового компьютера. Имя компьютера должно совпадать с именем реальной машины. Во второй панели укажите группу из п.3.



6. Зайдите на добавляемый компьютер, используя учетную запись локального администратора. Для этого установим Windows 7.

7. Выбираем созданную машину в списке и ждем «Запустить». После загрузки установочных файлов откроется окно с выбором языка. Оставляем по умолчанию и нажимаем Далее.

8. Далее нажимаем «Установить» и принимаем условия лицензии.

9. Затем выбираем «Полная установка».

10. В следующем окне вы увидите список доступных разделов диска. У вас будет один неразмеченный раздел (или уже созданный). Выберите его и нажмите «Далее».

11. Во время установки машина несколько раз автоматически перезагрузится. После всех перезагрузок вводим желаемое имя пользователя и компьютера.

12. Далее устанавливаем пароль для Вашей учетной записи.

13. Попускаем ввод ключа и нажимаем далее.

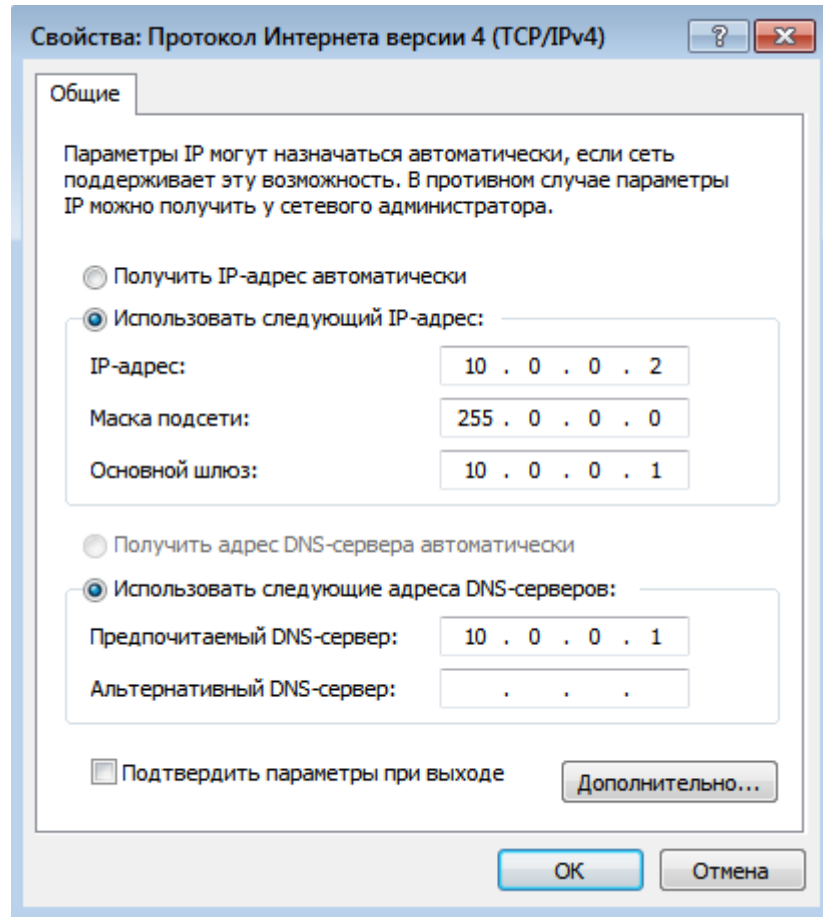
14. Откроется окно «**Центр обновления Windows**». Для виртуальной машины в учебных целях выберите третий вариант: «Отложить решение».

15. Установите текущий часовой пояс (например, (UTC+03:00) Москва, Санкт-Петербург) и проверьте дату/время. Нажмите «Далее».

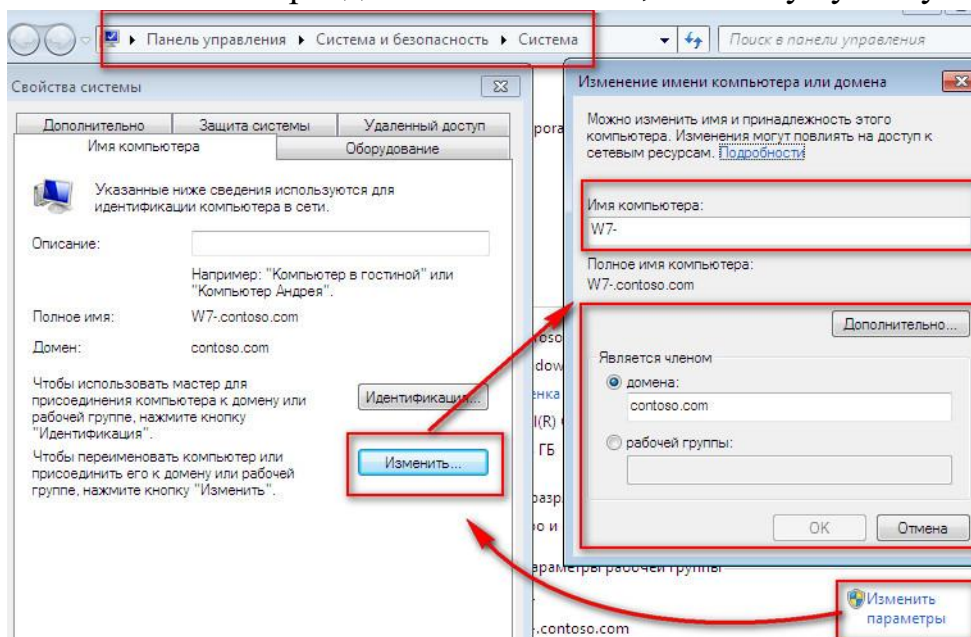
16. Появится окно выбора сетевого расположения. Выберите «Домашняя сеть».

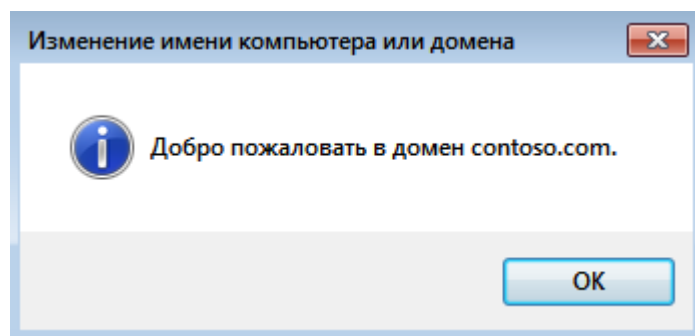
17. Виртуальная машина автоматически перезагрузится (или выйдет на экран приветствия).

18. На клиентской машине (Windows 7) установите следующие параметры сети IPv4



19. Откройте свойства компьютера -> изменение параметров
Внести компьютер в домен contoso.com, используя учетную запись test.





20. Для завершения операции необходимо перезагрузить компьютер.

3. Проверка работы доменной аутентификации

Убедиться, что компьютер успешно прошел аутентификацию в домене и пользователи могут входить под своими доменными учетными записями.

Упражнение 1. Вход в систему под учетной записью доменного пользователя

После перезагрузки компьютера SERVER02 выполните следующие действия:

1. На экране приветствия нажмите кнопку «Сменить пользователя» или выберите пункт «Другой пользователь».
2. Введите учетные данные доменного пользователя:
 - Имя пользователя: CONTOSO\User1 (или просто User1)
 - Пароль: (пароль, который вы задали при создании пользователя в Active Directory)

Важно: Обратите внимание на формат имени пользователя. Можно использовать:

- CONTOSO\User1 — полное доменное имя (NetBIOS-формат)
 - User1 — если компьютер автоматически подставит домен по умолчанию
3. Оставаясь под учетной записью CONTOSO\User1, откройте Проводник.
 4. В адресной строке введите путь: [\\SERVER01\Sales](#). Нажмите Enter.
 5. Вы увидите содержимое папки Sales, включая текстовый файл, который вы создали в упражнении 1.
 - 5.1. Попробуйте открыть текстовый файл — это должно сработать (права на чтение).
 - 5.2. Попробуйте создать новый файл в папке — система выдаст ошибку «Нет доступа».