Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ   
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

|  |  |
| --- | --- |
| Факультет | информационных технологий и управления |
| Кафедра | информационных технологий автоматизированных систем |

Лабораторная работа №4

**СОЗДАНИЕ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ И ГРУПП. УПРАВЛЕНИЕ РАБОЧЕЙ СРЕДОЙ ПОЛЬЗОВАТЕЛЕЙ**

|  |  |
| --- | --- |
| Выполнили: | Проверил: |
| студентки  группы №820605  Наумчик Д.С.  Прадед М.О.  Трофимчик Н.В. | Ярмолик В.И. |

Минск 2021

1. **Цель работы:**

Освоение технологии создания учетных записей пользователей и групп и управления рабочей средой пользователей.

1. **Описание процедур создания учетных записей профилей и рабочей среды пользователей.**

Операционные системы *Windows* *Server* устанавливаются с локальными учетными записями по умолчанию. Кроме того, вы можете создавать учетные записи пользователей, чтобы соответствовать требованиям вашей организации.

**Локальные учетные записи по умолчанию в *Active* *Directory***

Локальные учетные записи по умолчанию – это встроенные учетные записи, которые создаются автоматически при установке контроллера домена *Windows* *Server* и при этом создается домен. Эти локальные учетные записи по умолчанию имеют аналоги в *Active* *Directory*. Эти учетные записи также имеют доступ на уровне домена и полностью отделены от локальных учетных записей по умолчанию для рядового или отдельного сервера.

Вы можете назначать права и разрешения локальным учетным записям по умолчанию на определенном контроллере домена и только на этом контроллере домена. Эти учетные записи являются локальными для домена. После установки локальных учетных записей по умолчанию они сохраняются в контейнере "Пользователи" в каталоге "Пользователи и компьютеры *Active* *Directory*". Лучше хранить локальные учетные записи по умолчанию в контейнере *User* и не пытаться переместить эти учетные записи, например, в другое подразделение.

Локальные учетные записи по умолчанию в контейнере *Users*: *Administrator*, *Guest* и *KRBTGT*.

В основном локальные учетные записи по умолчанию делают следующее:

* Позволяют домену представлять, идентифицировать и аутентификацию удостоверения пользователя, назначенного учетной записи, используя уникальные учетные данные (имя пользователя и пароль). Для обеспечения максимальной безопасности каждому пользователю лучше назначить одну учетную запись. Нескольким пользователям не разрешено использовать одну учетную запись. Учетная запись пользователя позволяет пользователю вникать в компьютеры, сети и домены с уникальным идентификатором, который может быть аутентификацией компьютера, сети или домена.
* Авторизируют (предоставить или запретить) доступ к ресурсам. После проверки подлинности учетных данных пользователя пользователь получает разрешение на доступ к сетевым и доменным ресурсам на основе явно ограниченных прав пользователя на ресурс.
* Аудит действий, которые проводятся с учетной записью пользователя.

Учетные записи пользователей и компьютеров *Active* *Directory* могут представлять физический объект, например компьютер или пользователя, или выступать в качестве выделенных учетных записей служб для некоторых приложений.

Каждая локализованная учетная запись по умолчанию автоматически присваивается группе безопасности, которая предварительно имеет соответствующие права и разрешения для выполнения определенных задач. Группы безопасности *Active* *Directory* собирают учетные записи пользователей, учетные записи компьютеров и другие группы в управляемые единицы.

**Учетная запись администратора**

Учетная запись администратора — это учетная запись по умолчанию, используемая во всех версиях операционной системы *Windows* на каждом компьютере и устройстве. Учетная запись администратора используется системным администратором для задач, которые требуют учетных данных администратора. Эту учетную запись нельзя удалить или заблокировать, но ее можно переименовать или отключить.

Учетная запись администратора предоставляет пользователю полный доступ (разрешения полного доступа) к файлам, каталогам, службам и другим ресурсам, которые находятся на этом локальном сервере. Учетную запись администратора можно использовать для создания локальных пользователей и назначения прав пользователей и разрешений на управление доступом. Администратор также может использоваться для управления локальными ресурсами в любое время, просто изменяя права и разрешения пользователей. Хотя файлы и каталоги могут быть временно защищены от учетной записи администратора, учетная запись администратора может в любое время управлять этими ресурсами, изменяя разрешения на доступ.

При установке *Active Directory* на первом контроллере домена в домене создается учетная запись администратора для *Active* *Directory*. Учетная запись администратора является наиболее мощной учетной записью в домене. Ему предоставляется доступ на всем домене и административные права на администрирование компьютера и домена, а также он обладает самыми широкими правами и разрешениями для домена. Во время установки человек, устанавливавший доменные службы *Active* *Directory* на компьютере, создает пароль для этой учетной записи.

**Гостевая учетная запись**

Гостевая учетная запись — это локализованная учетная запись по умолчанию, которая имеет ограниченный доступ к компьютеру и по умолчанию отключена. По умолчанию пароль гостевой учетной записи остается пустым. Пустой пароль позволяет получить доступ к гостевой учетной записи без необходимости ввода пароля пользователем.

Гостевая учетная запись позволяет случайным или разовым пользователям, у которых нет отдельной учетной записи на компьютере, войти на локальный сервер или в домен с ограниченными правами и разрешениями. Гостевую учетную запись можно включить, а пароль можно настроить при необходимости, но только членом группы администраторов в домене.

**Учетная запись *KRBTGT***

Учетная запись *KRBTGT* является локальной учетной записью по умолчанию, которая выступает в качестве учетной записи службы центра распространения ключей (*KDC*). Эту учетную запись нельзя удалить, а имя учетной записи нельзя изменить. Учетную запись *KRBTGT* нельзя включить в *Active* *Directory*.

Проверка подлинности *Windows* *Server* *Kerberos* достигается с помощью специального билета *kerberos*, который шифруется симметричным ключом. Этот ключ является производным от пароля сервера или службы, к которой запрашивается доступ. Пароль *TGT* учетной записи *KRBTGT* известен только службе *Kerberos*. Для запроса билета сеанса *TGT* должен быть представлен в *KDC*. *TGT* выдан клиенту Kerberos из *KDC*.

**Управление локальными учетной записью по умолчанию в *Active* *Directory***

После установки локальных учетных записей по умолчанию эти учетные записи находятся в контейнере "Пользователи" в службе "Пользователи и компьютеры *Active* *Directory*". Локальные учетные записи по умолчанию можно создавать, отключать, сбрасывать и удалять с помощью консоли управления (*MMC*) пользователей и компьютеров *Active* *Directory*, а также с помощью средств командной строки.

Пользователи и компьютеры *Active* *Directory* можно использовать для назначения прав и разрешений определенному локальному контроллеру домена и только этому контроллеру домена, чтобы ограничить возможность локальных пользователей и групп выполнять определенные действия. Право разрешает пользователю выполнять определенные действия на компьютере, такие как архивирование файлов и папок или завершение работы компьютера. С другой стороны, разрешение на доступ — это правило, связанное с объектом, как правило, файлом, папкой или принтером, которое регулирует, какие пользователи могут иметь доступ к объекту и каким образом.

**Установка административных рабочих станций в домене и блокировка доступа к Интернету и электронной почте**

* 1. Как администратор домена на контроллере домена откройте "Пользователи и компьютеры *Active* *Directory*" и создайте новое *OU* для административных рабочих станций.
  2. Создайте учетные записи компьютеров для новых рабочих станций.
  3. Закроем компьютеры и пользователей *Active* *Directory*.
  4. Запустите консоль управления групповыми политиками (*GPMC*).
  5. Щелкните правой кнопкой мыши новое *OU* и создайте в этом домене > Создать *GPO* и привязать его сюда.
  6. Назовем *GPO* и > *ОК*.
  7. Раскройте *GPO*, щелкните правой кнопкой мыши новый *GPO* и выберите > "Изменить".
  8. Настройте, какие члены учетных записей могут локально выполнять вход на эти административные рабочие станции, следующим образом:
     1. Перейдите в "Конфигурация компьютера\Политики\Параметры *Windows*\Локальные политики" и щелкните "Назначение прав пользователя".
     2. Дважды щелкните "Разрешить вход локально" и выберите "Определить эти параметры политики".
     3. Нажмите кнопку "Добавить пользователя или группу" и введите "Администраторы предприятия" и "*ОК*".
     4. Нажмите кнопку "Добавить пользователя или группу" и введите "Администраторы домена" и "ОК". > \*\*\*\*
     5. Нажмите кнопку "Добавить пользователя или группу", введите "Администраторы" и "*ОК*".
  9. Настройте конфигурацию прокси-сервера:
     1. Перейдите к параметрам конфигурации пользователя\*Policies\Windows Settings\Internet Explorer > Connection.*
     2. Дважды щелкните "Параметры прокси-сервера", выберите "Включить параметры прокси-сервера", введите 127.0.0.1 (*IP*-адрес сетевого цикла) в качестве прокси-адреса и *ОК*.
  10. Настройте режим обработки с перекатом, чтобы параметр прокси-сервера групповой политики пользователя применялся к всем пользователям на компьютере следующим образом:
      1. Перейдите в меню "Конфигурация компьютера\Политики\Административные шаблоны\Система" > "Групповая политика".
      2. Дважды щелкните режим обработки политики обратной политики пользовательской групповой политики > Включить.
      3. Выберите режим объединения > *ОК*.
  11. Настройте обновления программного обеспечения следующим образом:
      1. Перейдите в меню "Конфигурация компьютера\Политики\Административные шаблоны\Компоненты *Windows*" и щелкните "*Windows* *Update*".
      2. Настройте параметры Обновления *Windows*
  12. Настройте входящий брандмауэр для блокировки всех подключений следующим образом:
      1. Щелкните правой кнопкой мыши брандмауэр *Windows* с расширенными *LDAP*://path свойствами.
      2. Убедитесь, что в каждом профиле включен брандмауэр и что входящие подключения настроены на блокировку всех подключений.
      3. Нажмите кнопку *ОК*, чтобы завершить настройку.
  13. Закройте консоль управления групповыми политиками.
  14. Установите операционную систему *Windows* на рабочих станциях, придайте каждой рабочей станции те же имена, что и учетным записям компьютеров, которые им назначены, а затем присоедините их к домену.

1. **Выводы по работе.**

Мы освоили технологии создания учетных записей пользователей и групп и управления рабочей средой пользователей.