



Домены и рабочая группа в ОС Windows

Понятия домен и рабочая группа

- **Домен** — это логическая группировка компьютеров, объединенных общей базой данных пользователей и компьютеров, политикой безопасности и управления
- **Рабочая группа** — это логическая группировка компьютеров, объединенных общим именем для облегчения навигации в пределах сети

Рабочая группа

- Каждый в рабочей группе пользователи равноправны и поддерживает собственную локальную базу данных учетных записей пользователей
- Отсюда вытекает основная проблема, которая не позволяет использовать рабочие группы в крупных корпоративных сетях.

Рабочая группа

- Действительно, вход в защищенную систему является обязательным, а непосредственный и сетевой входы принципиально различаются (непосредственный контролируется локальным компьютером, а сетевой — удаленным), то, например, пользователю, вошедшему на компьютер Comp1 под локальной учетной записью User1, будет отказано в доступе к принтеру, установленному на компьютере Comp2, поскольку в его локальной базе нет пользователя с именем User1
- Для обеспечения «прозрачного» взаимодействия в рабочей группе нужно создавать одинаковые учетные записи с одинаковыми паролями на всех компьютерах, где работают пользователи и расположены ресурсы.

Рабочая группа

- В ОС Windows для рабочих групп предусмотрен специальный режим: «Использовать простой общий доступ к файлам», позволяющий обойти указанную проблему (данный режим включен по умолчанию).
- В этом случае подключение к любому сетевому компьютеру осуществляется от имени его локальной гостевой учетной записи, которая включается с помощью Мастера настройки сети (по умолчанию она отключена) и для которой настраивается нужный уровень доступа.
- Для ОС Windows версии Home Edition этот способ сетевого взаимодействия является основным и отключить его нельзя (поэтому компьютеры с данной ОС невозможно сделать участниками домена).
- Понятно, что управлять учетными записями и ресурсами в рабочей группе можно только при небольшом количестве компьютеров и пользователей.
- В крупных сетях следует применять домены

Домен

- Домены создаются на основе сетевых ОС Windows, а база данных, поддерживается контроллерами домена.
- Важным в доменах является то, что все компьютеры здесь не сами осуществляют проверку пользователей при входе, а передоверяют эту процедуру контроллерам.
- Такая организация доступа позволяет легко осуществить однократную проверку пользователя при входе в сеть, а затем уже без проверки предоставлять ему доступ к ресурсам всех компьютеров домена.

Домен Windows

- Это, по сути, сеть управляемых компьютеров, используемых в бизнес-среде. По крайней мере, один сервер, называемый **контроллер домена**, отвечает за другие устройства.
- Это позволяет сетевым администраторам (обычно ИТ-персоналу) управлять компьютерами в домене с помощью пользователей, настроек и многого другого.

Домен Windows

- Поскольку домены предназначены не для домашних пользователей, только для Windows версии Professional или Enterprise
- Для управления доменом потребуется копия Windows Server для контроллера домена, поскольку она включает в себя необходимое программное обеспечение, такое как Active Directory

Проверка компьютера на наличие домена

- Чтобы проверить, является ли ваш компьютер частью домена, откройте **Панель управления** и нажмите **система** запись. Заглянуть под **Имя компьютера** раздел. Если вы видите **Workgroup** вход с **РАБОЧАЯ** (по умолчанию) или другое имя в списке, ваш компьютер не находится в домене. Точно так же, если вы видите **Домен** здесь, то ваш компьютер находится в домене.
- Эти шаги также позволяют вам найти ваше доменное имя на вашем компьютере.

Домены против рабочих групп

- Если компьютер не принадлежит домену, он входит в рабочую группу
- Рабочие группы гораздо более слабые, чем домены, поскольку у них нет центральной власти. У каждого компьютера свои правила.
- В современных версиях Windows рабочие группы на самом деле являются формальностью, особенно когда Microsoft отказывается от функции HomeGroup

Домены против рабочих групп

- Windows никогда не просит вас настроить один, и они используются только для обмена файлами между устройствами в вашей сети, Microsoft хочет, чтобы вы использовали OneDrive для этого в настоящее время, поэтому, если вы не хотите настраивать свою собственную рабочую группу, вам не нужно беспокоиться об этом.


Control Panel Home

- Device Manager
- Remote settings
- System protection
- Advanced system settings

See also

- Action Center
- Windows Update
- Performance Information and Tools

reserved.



System

Rating:	5.9 Windows Experience Index
Processor:	Intel(R) Core(TM)2 Quad CPU @ 2.40GHz 2.40 GHz
Installed memory (RAM):	8.00 GB
System type:	64-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:	Turbine	Change settings
Full computer name:	Turbine	
Computer description:		
Workgroup:	WORKGROUP	

System Properties

Computer Name Hardware Advanced System Protection Remote



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name:

Turbine

Workgroup:

WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

Network ID...

To rename this computer or change its domain or workgroup, click Change.

Change...

OK

Cancel

Apply



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

[More information](#)

Computer name:

Turbine

Full computer name:

Turbine

More...

Member of

Domain:

redmond.corp.microsoft.com

Workgroup:

WORKGROUP

OK

Cancel

Учетная запись пользователя домена

- В отличие от персонального компьютера, подключенный к домену ПК не использует локальные учетные записи
- Вместо этого контроллер домена управляет логинами. Используя Microsoft Active Directory, программное обеспечение для управления пользователями, сетевые администраторы могут легко создавать новых пользователей и отключать старых. Они также могут добавлять пользователей в определенные группы, чтобы разрешить доступ к частным папкам сервера.

Учетная запись пользователя домена

- С помощью доменной учетной записи вы можете войти на любой компьютер в домене. Вы начнете с новой учетной записи на этом компьютере, но это позволит вам использовать любой компьютер в вашей компании при необходимости. Благодаря учетным записям домена бывшие сотрудники не могут войти в систему. Если они попытаются войти со своим старым паролем, они увидят сообщение, что им отказано в доступе.
- Экран входа в Windows выглядит немного иначе, когда вы используете компьютер, подключенный к домену. Вместо локального имени пользователя вам необходимо убедиться, что вы входите в домен под своим именем пользователя.

Контроль домена и групповая политика в Windows


- Самым большим преимуществом доменов является простота управления несколькими компьютерами одновременно. Без домена ИТ-персоналу пришлось бы индивидуально управлять каждым компьютером в компании.
- Это означает настройку параметров безопасности, установку программного обеспечения и управление учетными записями пользователей вручную. Хотя это может работать для крошечной компании, это не масштабируемый подход, и он быстро станет неуправляемым.

Контроль домена и групповая политика в Windows

- Наряду с управлением пользователями Active Directory присоединение компьютеров к домену позволяет использовать групповую политику.
- Используя контроллер домена, администраторы могут настраивать все виды безопасности и использовать политики для всех компьютеров. Например, групповая политика упрощает применение всех следующих методов: удаление элементов из меню «Пуск», остановить пользователей от изменения параметров подключения к интернету, блокировка командной строки, перенаправьте определенную папку, чтобы использовать ее на сервере, запретить пользователю изменять звуки, подключить принтер к новым компьютерам автоматически
- Это лишь небольшая часть того, что позволяет групповая политика. Администраторы могут настроить эти изменения один раз и применить их ко всем компьютерам, даже к новым, которые они настроят позже.

Присоединиться к домену в Windows

- Панель управления > Система.
- На **Имя компьютера, домен и параметры рабочей группы** страницу, нажмите **Изменить настройки**.
- Вы увидите **Свойства системы** окно. Нажмите на **+** **Изменить** кнопка рядом с **Чтобы переименовать этот компьютер или изменить его домен**.
- После перезагрузки ПК ваш компьютер будет находиться в домене. Чтобы покинуть домен, повторите этот процесс, но выберите **Workgroup** вместо пузыря.
- Конечно, для этого вам понадобится пароль администратора домена

- 
- По сути, домены позволяют администраторам контролировать большое количество бизнес-ПК из центрального местоположения.
 - Локальный пользователь имеет меньший контроль над управляемым доменом ПК, чем персональный.
 - Без доменов управление корпоративными компьютерами было бы кошмаром для ИТ-персонала.

Рабочая группа Windows

- **Рабочая группа Windows** (на английском языке **Workgroup**) является функцией операционных систем Microsoft. На практике это набор компьютеров, подключенных к сети, и его функция заключается в том, чтобы заложить основы, необходимые для обмена файлами и принтерами между ПК.
- Компьютер, являющийся членом рабочей группы, может разрешить другому компьютеру, являющемуся членом той же группы, доступ к своим общим ресурсам. Компьютеры, которые являются членами разных рабочих групп, но принадлежащих к одной локальной сети, могут напрямую получать доступ к общим ресурсам в группе, к которой они принадлежат.
- Рабочая группа присутствует на всех компьютерах с Windows 10, Windows 8.1/8, Windows 7 и Windows Vista

Разница между рабочей группой и доменом

- *Заключается в способе управления компьютерами и сетевыми ресурсами.*
- Обычно компьютеры корпоративной или большой сети являются частью домена, в то время как компьютеры домашней сети являются частью рабочей группы, а часто и домашней группы (→ что такое домашняя группа).

Функции рабочей группы Windows

- Для доступа к общим элементам на компьютере рабочей группы Windows у вас должна быть учетная запись на том же компьютере.
- Предположим, что пользователь **Boris** с **White PC** (принадлежащего **Рабочей группе: WORKGROUP**) хочет получить доступ к файлу с именем **Person** на **Black PC** (также принадлежащему **Рабочей группе: WORKGROUP**). Чтобы получить доступ к *личному файлу*, как на белом ПК, так и на черном ПК, должна присутствовать учетная запись пользователя **Boris**.
- Рабочая группа всегда идентифицируется по имени.
- По умолчанию на этапе установки операционной системы Windows автоматически создает **рабочую группу** с именем **WORKGROUP**.

Важно

- Если компьютер является членом домена, перед добавлением в рабочую группу он будет удален из домена и соответствующая учетная запись будет деактивирована.
- Имя Рабочей группы может быть длиной до 15 символов и не должно содержать символов * () = + _ [] <> \ | / ; : ' » , <> ?

Является членом

домена:


рабочей группы:

OK

Отмена



Создание групп в Active Directory

- 
- Группы содержат элементы (пользователей, компьютеры, другие группы), управление которыми осуществляется как одним объектом.
 - В Windows Server существует семь типов групп- две группы доменов с тремя областями действий в каждой и локальная группа безопасности.


Существует два типа групп - безопасности и распространения

- **Группа распространения** - применяется для создания групп почтовых рассылок. Письмо отправленное на группу распространения дойдет всем пользователям группы. Это группа не предназначена для работы с предоставлением доступа на ресурсы.
- **Группа безопасности** - применяется для управления безопасностью доступа к ресурсам. Т.е. если вы хотите для сетевой папки создать группу, для этого необходимо создать группу безопасности. Так же с помощью группы безопасности можно сделать почтовую рассылку, но это не рекомендуется делать поскольку для этого есть группа распространения.

Помимо групп существует три области действия для каждой группы

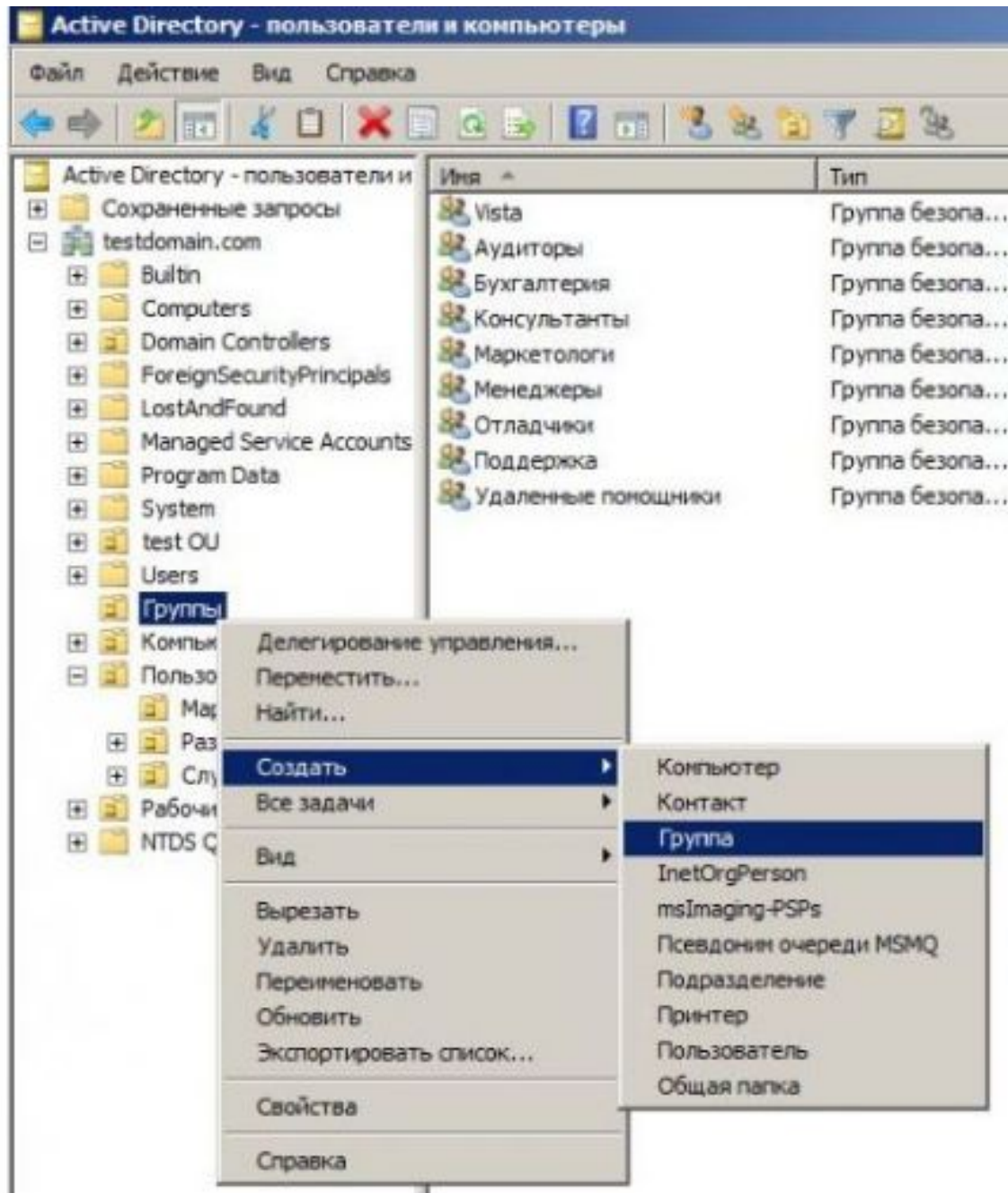
- **Локальная в домене** - используется для управления разрешениями доступа к ресурсам в пределах всего домена.
- **Глобальная группа** - используется для определение коллекции объектов доменов на основании бизнес-правил и управление объектами, которые требуют ежедневного использования.
- **Универсальная группа** - Рекомендуется использовать в лесах из множество доменов. С помощью нее можно определять роли и управлять ресурсами, которые распределены на нескольких доменах.

Область действия группы	Члены группы из того же домена	Члены группы из другого домена в том же лесу	Члены группы из доверенного домена	Группе могут быть назначены разрешения в...	Область действия группы можно преобразовать в...
Локальная в домене	<ul style="list-style-type: none"> - Пользователи - Компьютеры - Глобальные группы - Локальные группы - Локальные группы 	<ul style="list-style-type: none"> - Пользователи - Компьютеры - Глобальные группы - Локальные группы 	<ul style="list-style-type: none"> - Пользователи - Компьютеры - Глобальные группы 	Разрешения члена могут быть назначены только в домене, которому принадлежит родительская локальная группа домена	- в универсальную в том случае, если эта группа не содержит другую локальную группу в домене в качестве члена;
Универсальная группа	<ul style="list-style-type: none"> - Пользователи - Компьютеры - Глобальные группы - Локальные группы 	<ul style="list-style-type: none"> - Пользователи - Компьютеры - Глобальные группы - Локальные группы 	Нет доступа	Любой домен или лес	<ul style="list-style-type: none"> - в глобальную в том случае, если эта группа не содержит в качестве члена другую универсальную группу; - в локальную группу в домене.
Глобальная группа	<ul style="list-style-type: none"> - Пользователи - Компьютеры - Глобальные группы 	Нет доступа	Нет доступа	Разрешения члена могут быть назначены в любом домене	- в универсальную в том случае, если изменяемая группа не является членом другой глобальной группы;


- 
- Локальная группа считается самой примитивной, так как она доступна только на одном компьютере. Такая группа создается в базе данных диспетчера безопасности учетных записей рядового компьютера и поэтому в домене управление локальными группами не нужно

Создание группы с помощью консоли **Active Directory- Пользователи и компьютеры**

- Для того что бы создать группу, необходимо запустить консоль **Active Directory- Пользователи и компьютеры**, зайти в необходимое подразделение нажать кнопку "**Создание новой группы в текущем контейнере**", в открывшемся окне **Новый объект- Группа** введите имя группы и выберите необходимый тип и область действия



Новый объект - Группа X

 Создать в: testdomain.com/Группы

Имя группы:

Имя группы (пред-Windows 2000):

Область действия группы

Локальная в домене

Глобальная

Универсальная

Тип группы

Группа безопасности

Группа распространения

Создание группы с помощью командной строки

- Для создания группы в командной строке служит команда `Dsadd`.
- Общий вид команды `Dsadd group DN_группы + дополнительные параметры`.
- **-secgrp**. Данный параметр указывает тип группы: безопасности (`yes`) или распространения (`no`). Если параметр не указан, то по умолчанию значением данного параметра считается `yes`;
- **-scope**. Текущий параметр задает область действия группы. Доступные параметры: локальная в домене (`l`), глобальная (`g`) или универсальная (`u`). По умолчанию, также как и при помощи графического интерфейса, область действия назначается глобальной;
- **-samid**. Этот параметр определяет использование для данной группы SAM имени, как уникального атрибута `sAMAccountName` группы. Желательно имя для `sAMAccountName` и группы указывать идентичные;
- **-desc**. Данный параметр отвечает за краткое описание группы;
- **-memberof**. Этот параметр назначает одну или несколько групп, к которым требуется добавить новую. Если групп несколько, то их следует добавлять через пробел;
- **-members**. При помощи этого параметра вы можете добавить членов в группу. Члены должны указываться в виде DN-имен и разделяться пробелами.
- Пример создания группы с помощью командной строки:
- **Dsadd group «CN=Администраторы,OU=Группы,DC=pk-help,DC=com» -secgrp yes -scope g -samid «Администраторы сети» -desc «Администраторы сети»**