**Содержание:**


# Групповая политика. Применение объектов групповой политики

Групповые политики являются одним из наиболее мощных инструментов управления пользователями и компьютерами в домене Active Directory. Однако, как и любой сложный инструмент, они требуют четкого понимания принципов своей работы и тщательного планирования. Без этого применение групповых политик может выдать не совсем тот результат, который  требуется.

Вот собственно о них, основных принципах, и пойдет речь в этой статье. И начнем мы с самого основного — области действия.

### Область действия групповых политик

Все групповые политики имеют свою область действия (scope), которая определяет границы влияния политики. Области действия групповых политик условно можно разделить на четыре типа.

### Локальные групповые политики

Групповые политики, применяемые к локальному компьютеру, или локальные групповые политики. Эти политики настраиваются в оснастке «Редактор локальных групповых политик» и применяются только к тому компьютеру, на котором они были настроены. Они не имеют механизма централизованного развертывания и управления и, по сути, не являются групповыми политиками.

### Групповые политики доменов

Объекты групповых политик, применяемые к домену Active Directory (AD) и оказывающие влияние на все объекты, имеющие отношение к данному домену. Поскольку в рамках домена работает механизм наследования, то все политики, назначенные на домен, последовательно применяются и ко всем нижестоящим контейнерам.

**Групповые политики подразделения**

Политики, применяемые к подразделению (OU) и оказывающие влияние на все содержимое данного OU и дочерних OU (при их наличии).

**Групповые политики сайтов**

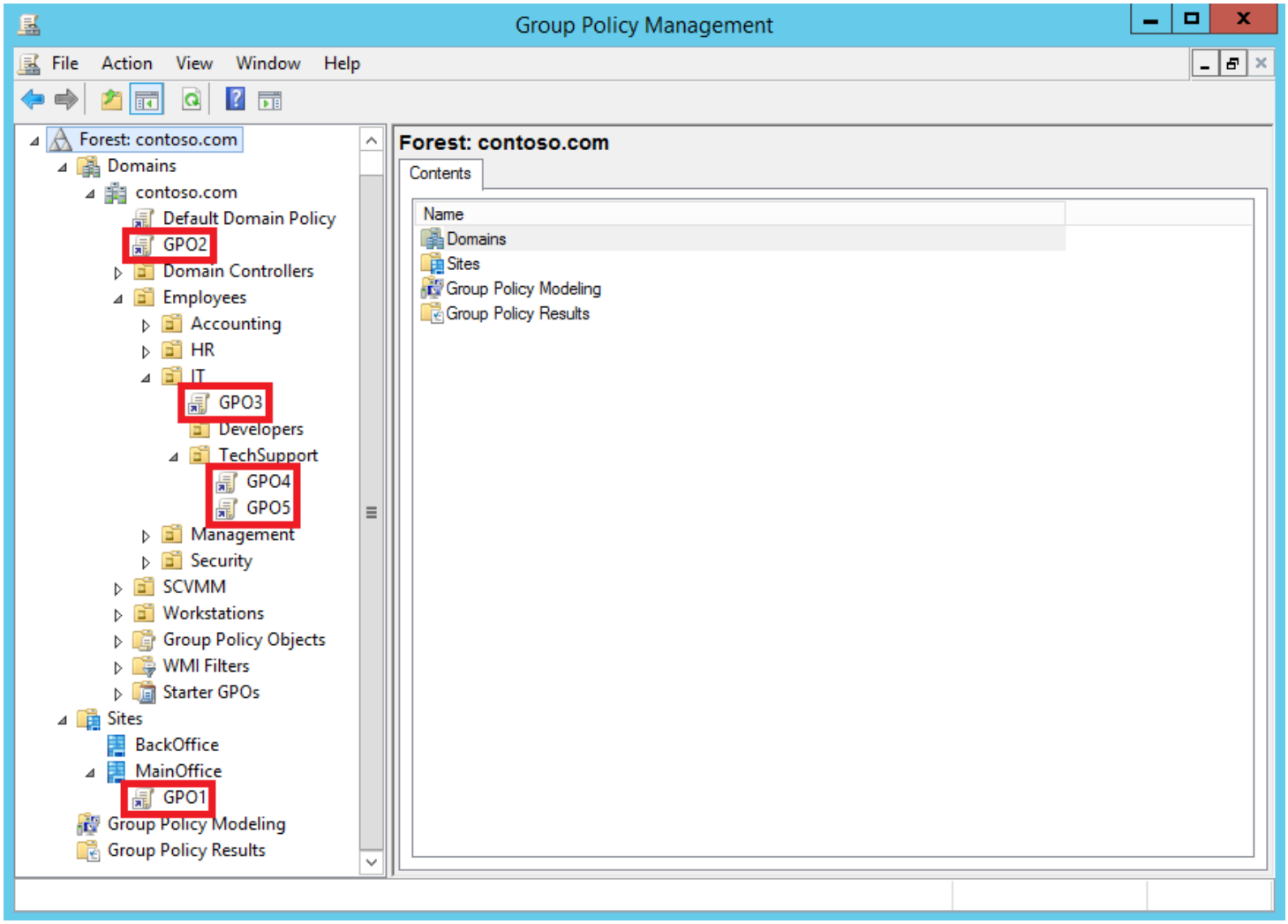
Напомню, что в отличие от доменов, которые представляют из себя логическую структуру организации, сайты в AD используются для представления ее физической структуры. Границы сайта определяются одной или несколькими IP-подсетями, которые объединены высокоскоростными каналами связи. В один сайт может входить несколько доменов и наоборот, один домен может содержать несколько сайтов.

Объекты групповой политики, примененные к сайту AD, оказывают влияние на все содержимое этого сайта. Следовательно, групповая политика, связанная с сайтом, применяется ко всем пользователям и компьютерам сайта независимо от того, к какому домену они принадлежат.

## Порядок применения групповых политик

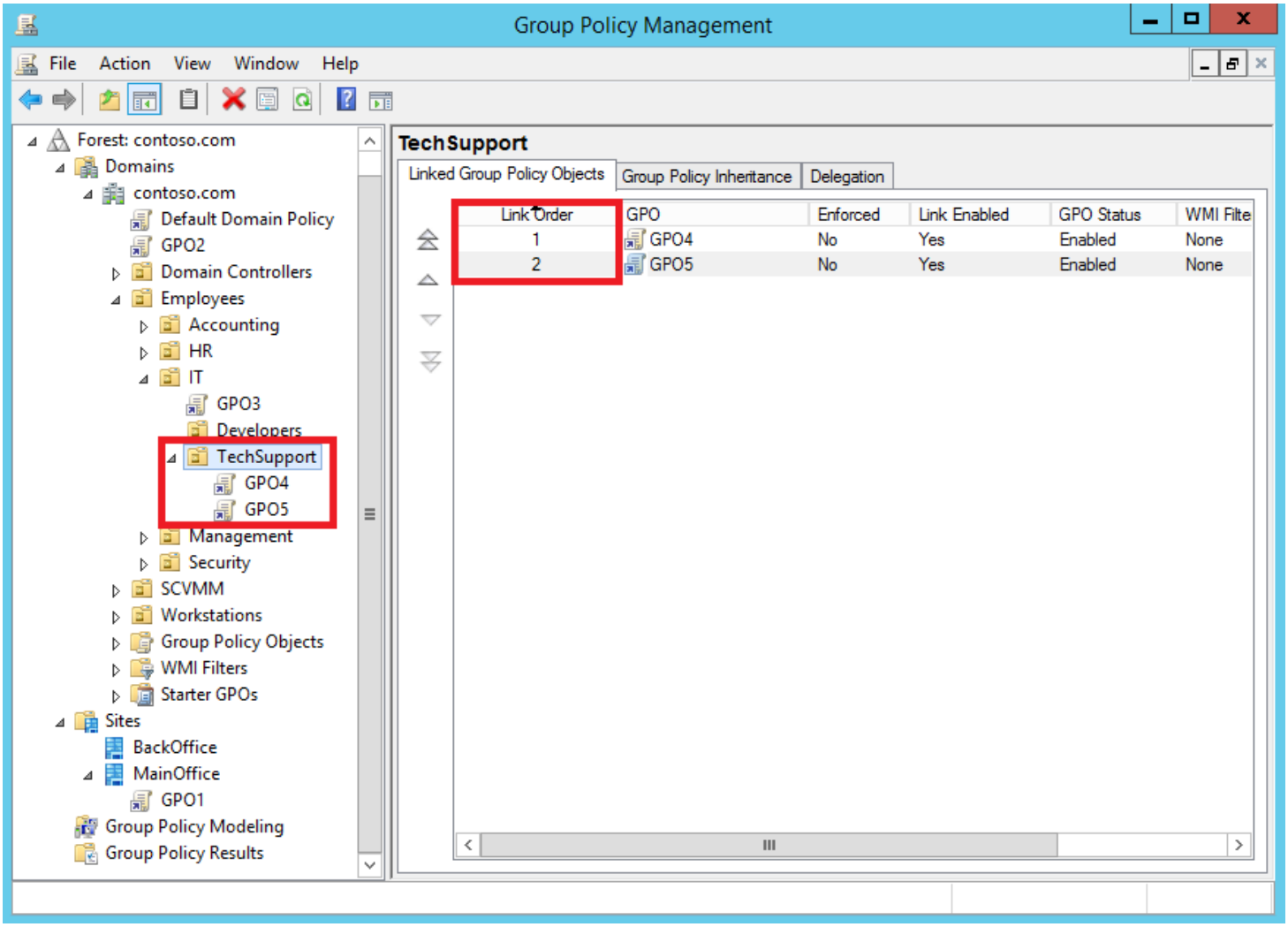
Порядок применения групповых политик напрямую зависит от их области действия. Первыми применяются локальные политики, затем политики, назначенные на сайт, затем отрабатывают доменные политики и затем политики, назначенные на OU.

Так в нашем примере (на рисунке ниже) сначала отработает локальная политика (условно назовем ее GPO0), затем политика сайта GPO1, затем политика домена GPO2, ну а затем применятся политики, назначенные на OU. При этом политики применяются в соответствии с иерархией — сначала политика GPO3, назначенная на вышестоящее OU, затем нижестоящие политики GPO4 и GPO5.




Если на одну OU назначено несколько GPO, то они обрабатываются в том порядке, в котором были назначены. Например, к подразделению TechSupport относятся GPO4 и GPO5, которые обрабатываются согласно порядку назначения (Link Order).

Политики обрабатываются в обратном порядке (снизу вверх), т.е. политика с номером 1 отработает последней. При необходимости этот порядок можно изменить, выделив политику и передвинув ее вверх или вниз с помощью соответствующих стрелок.



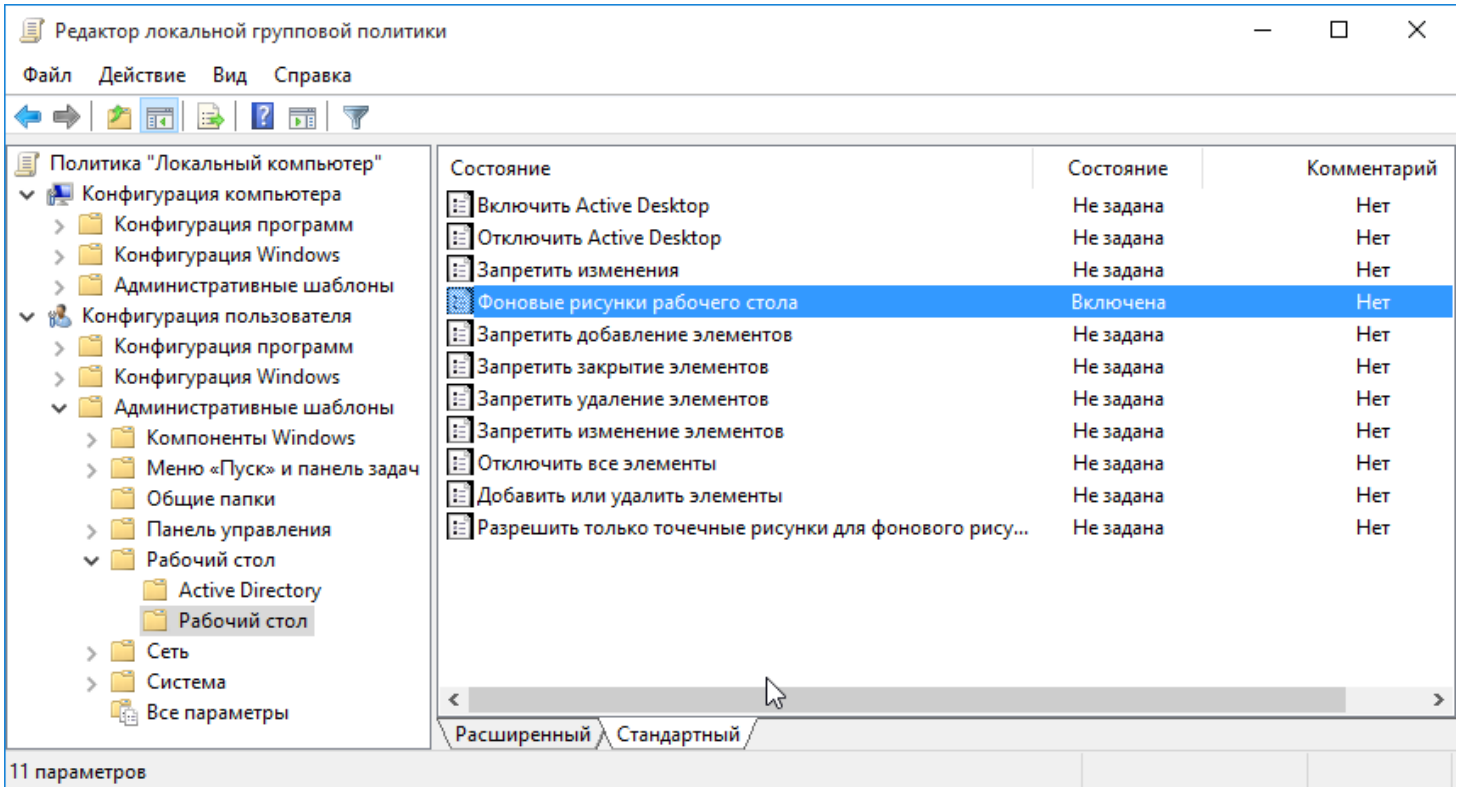

# Приоритет групповых политик

Приоритет GPO напрямую зависит от порядка их применения — чем позднее применяется политика, тем выше ее приоритет. При этом нижестоящие политики могут переопределять вышестоящие — например локальная политика GPO0 будет переопределена доменной политикой сайта GPO1, доменая политика GPO2 — политикой GPO3, а политика вышестоящего GPO3 — нижестоящими политиками GPO4 и GPO5.

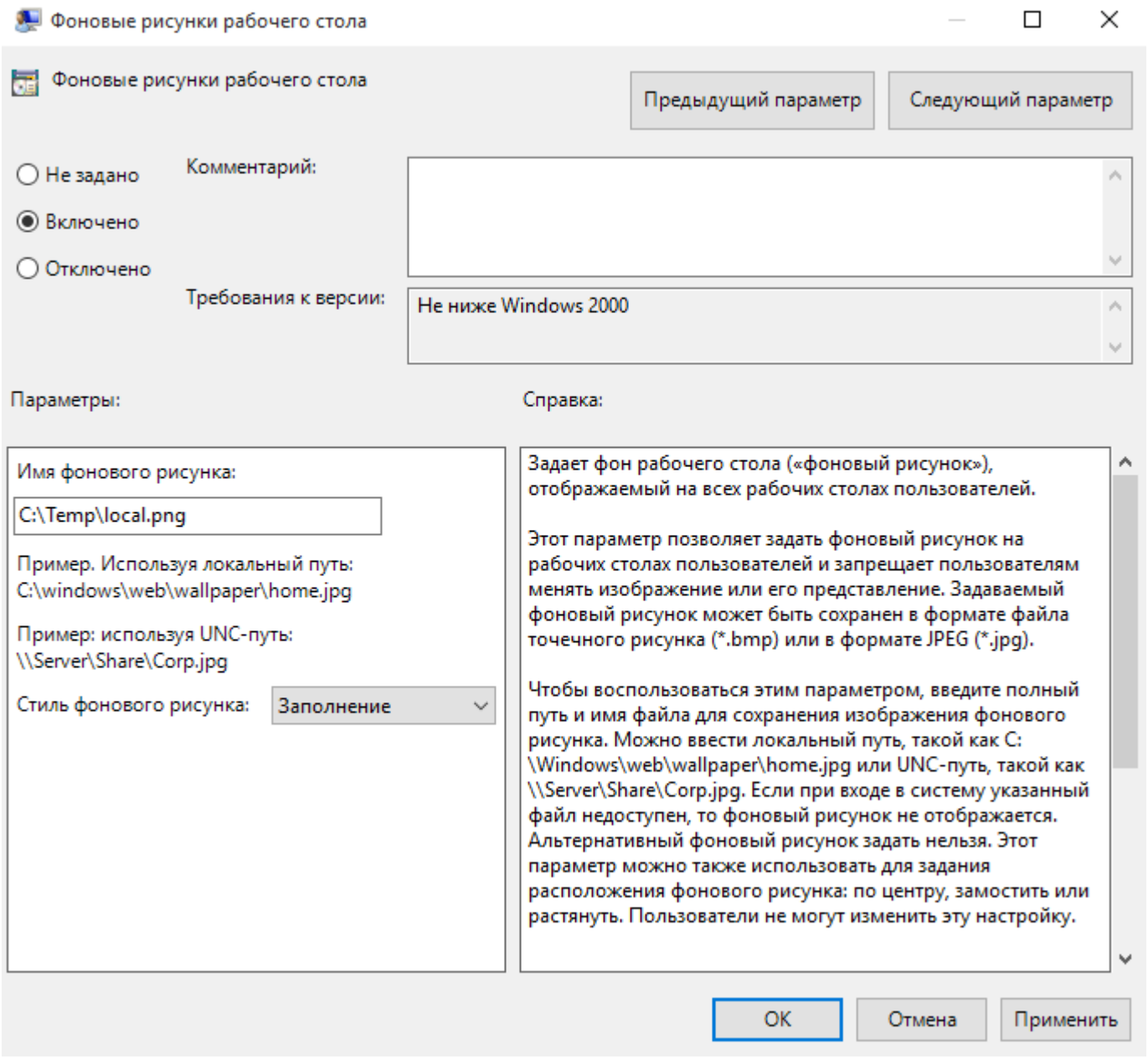
Для большей наглядности проведем эксперимент. Для проверки действия политик будем заходить на рабочую станцию WKS1 под учетной записью пользователя Kirill, находящегося в OU TechSupport.

На рабочей станции WKS1 открываем редактор локальных групповых политик (gpedit.msc) и переходим в раздел Конфигурация пользователя\Административные

шаблоны\Рабочий стол\Рабочий стол (User Configuration\Administrative Template\Desktop\Desktop).

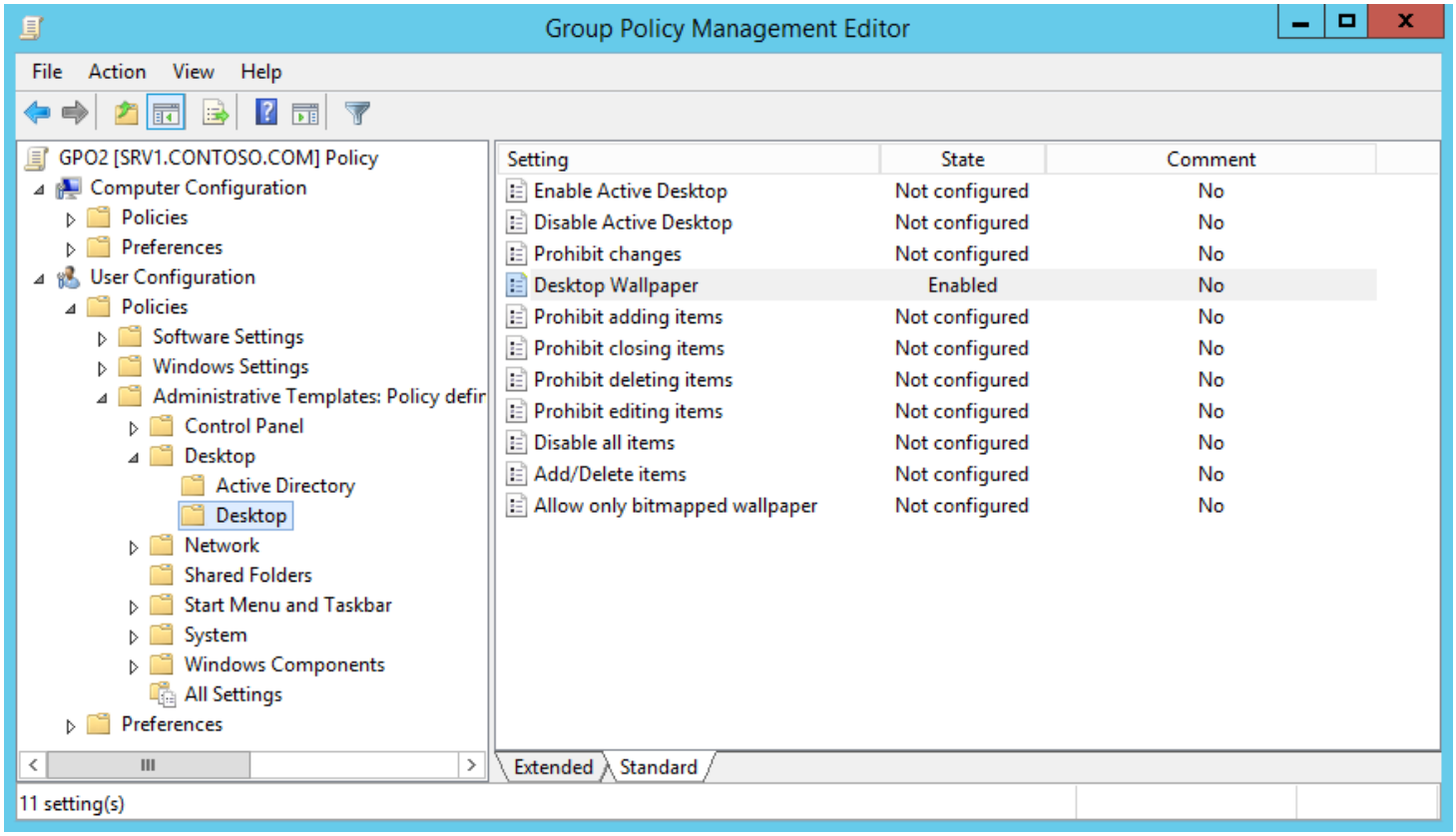



Откроем политику Фоновые рисунки рабочего стола (Desktop Wallpaper) и укажем использовать в качестве обоев изображение local.png.

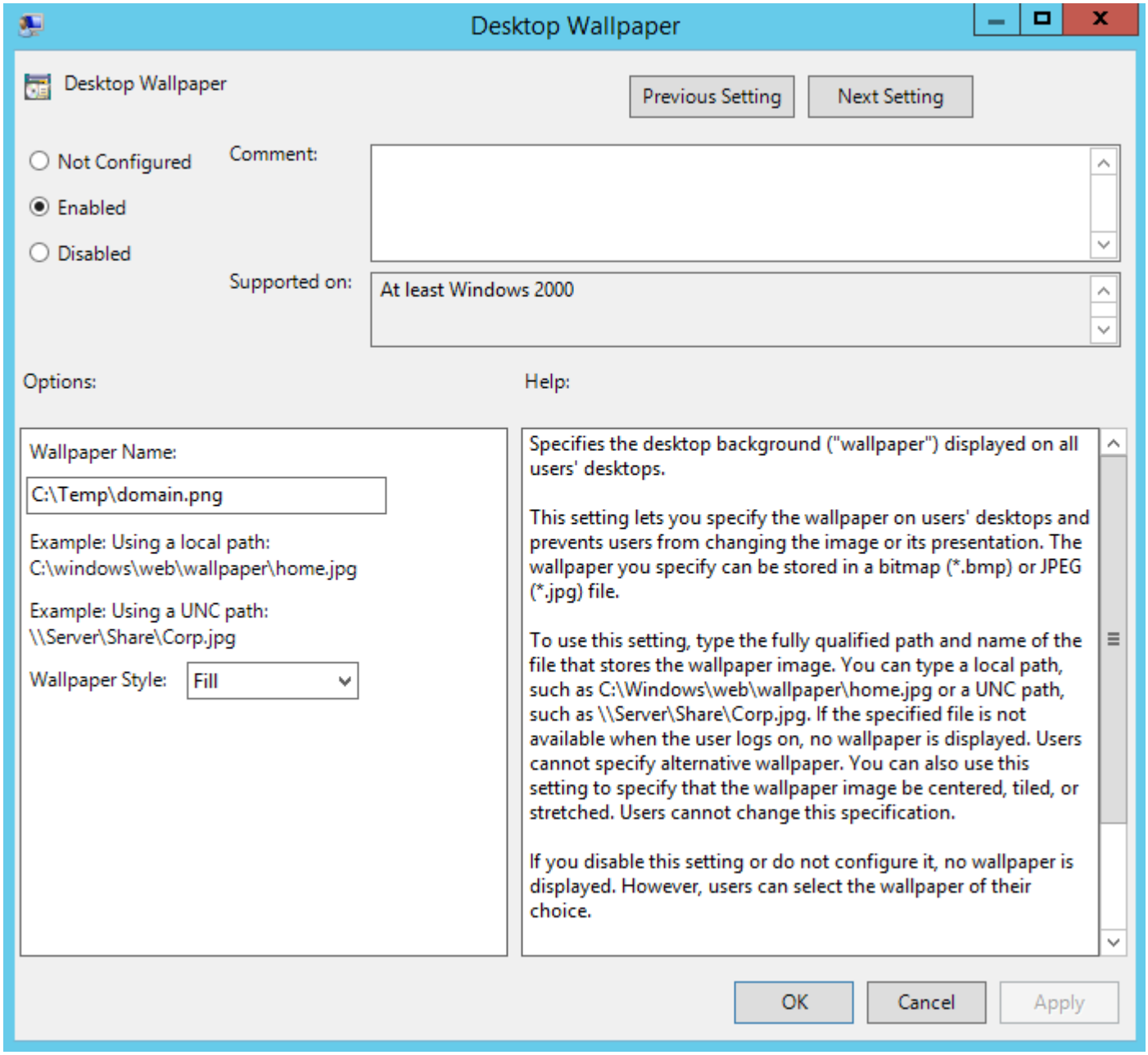



Затем перелогиниваемся и проверяем, что политика отработала и обои изменены.

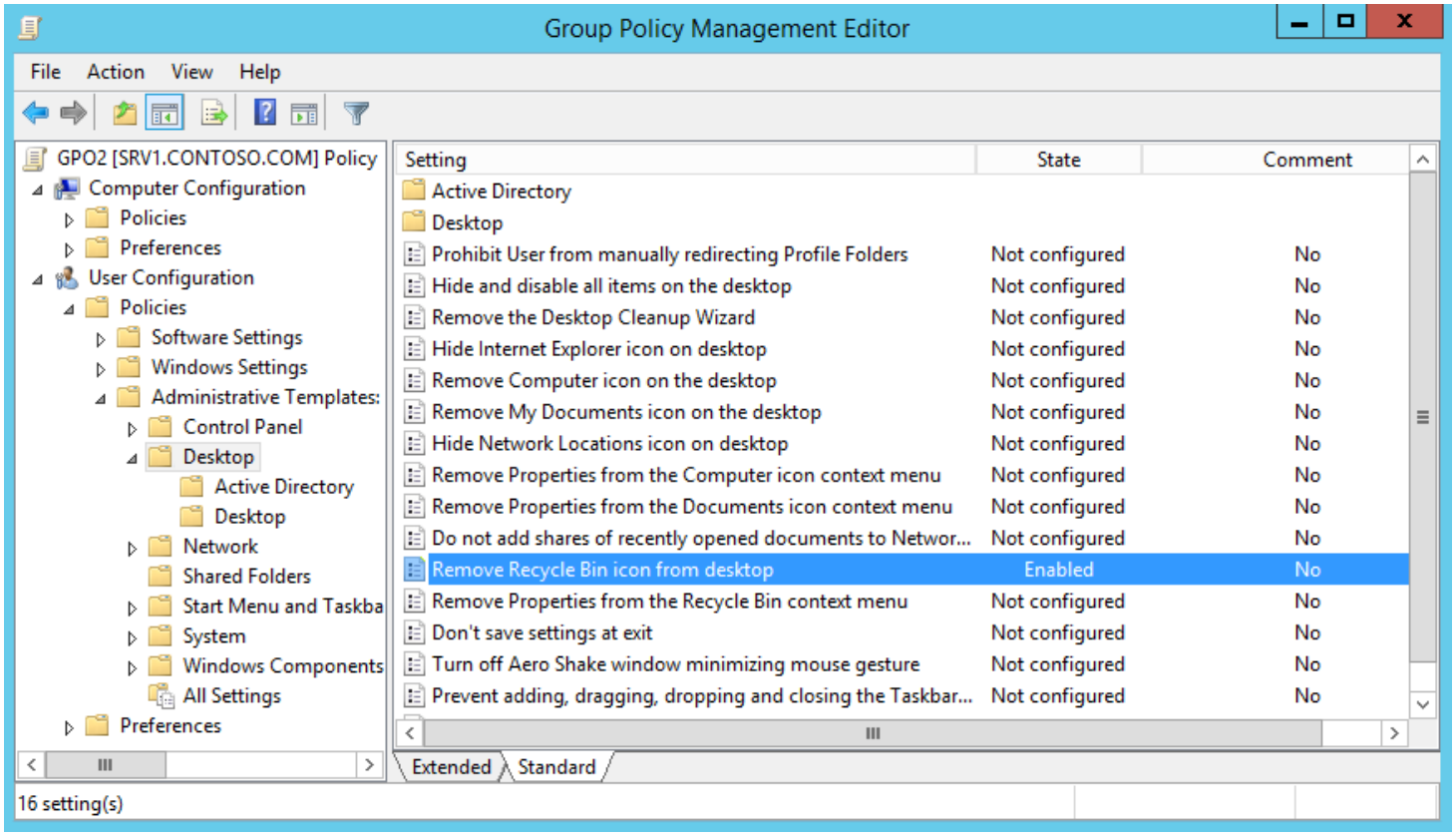
Следующим шагом будет настройка доменной политики. Для этого в оснастке «Group Policy Management» выбираем политику GPO2 и открываем ее для редактирования.

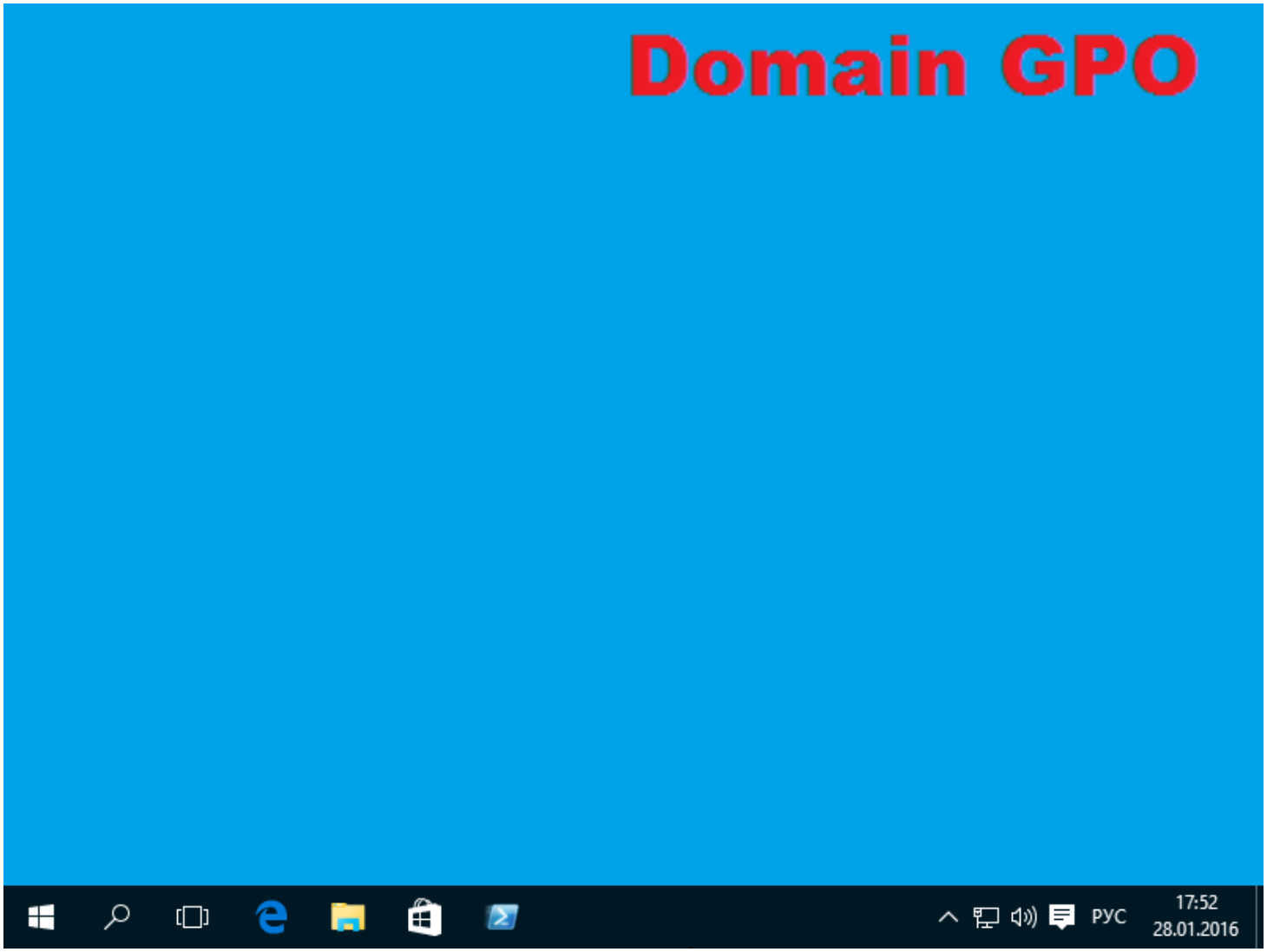



Находим политику, отвечающую за смену обоев и устанавливаем в качестве рисунка рабочего стола изображение domain.png.



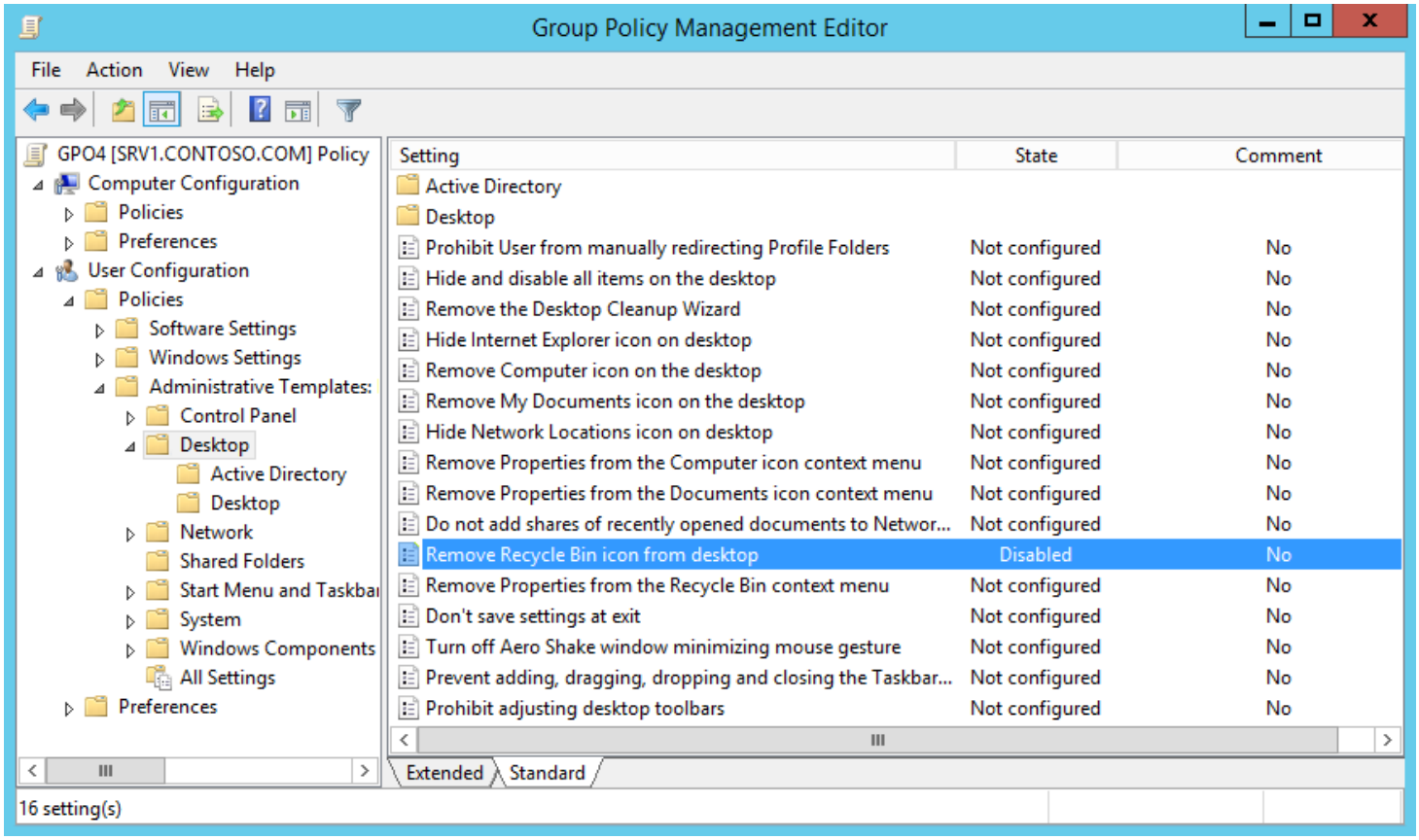

Дополнительно переходим в раздел выше и включаем политику «Remove Recycle Bin icon from desktop», удаляющую корзину с рабочего стола.


Group Policy Management Editor
File
Action
View
Help
GPO2 [SRV1.CONTOSO.COM] Policy
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Administrative Templates:
Control Panel
Desktop
Active Directory
Desktop
Network
Shared Folders
Start Menu and Taskba
System
Windows Components
All Settings
Preferences
Setting
State
Comment
Active Directory
Desktop
Prohibit User from manually redirecting Profile Folders
Not configured
No
Hide and disable all items on the desktop
Not configured
No
Remove the Desktop Cleanup Wizard
Not configured
No
Hide Internet Explorer icon on desktop
Not configured
No
Remove Computer icon on the desktop
Not configured
No
Remove My Documents icon on the desktop
Not configured
No
Hide Network Locations icon on desktop
Not configured
No
Remove Properties from the Computer icon context menu
Not configured
No
Remove Properties from the Documents icon context menu
Not configured
No
Do not add shares of recently opened documents to Networ...
Not configured
No
Remove Recycle Bin icon from desktop
Enabled
No
Remove Properties from the Recycle Bin context menu
Not configured
No
Don't save settings at exit
Not configured
No
Turn off Aero Shake window minimizing mouse gesture
Not configured
No
Prevent adding, dragging, dropping and closing the Taskbar...
Not configured
No
Extended
Standard
16 setting(s)

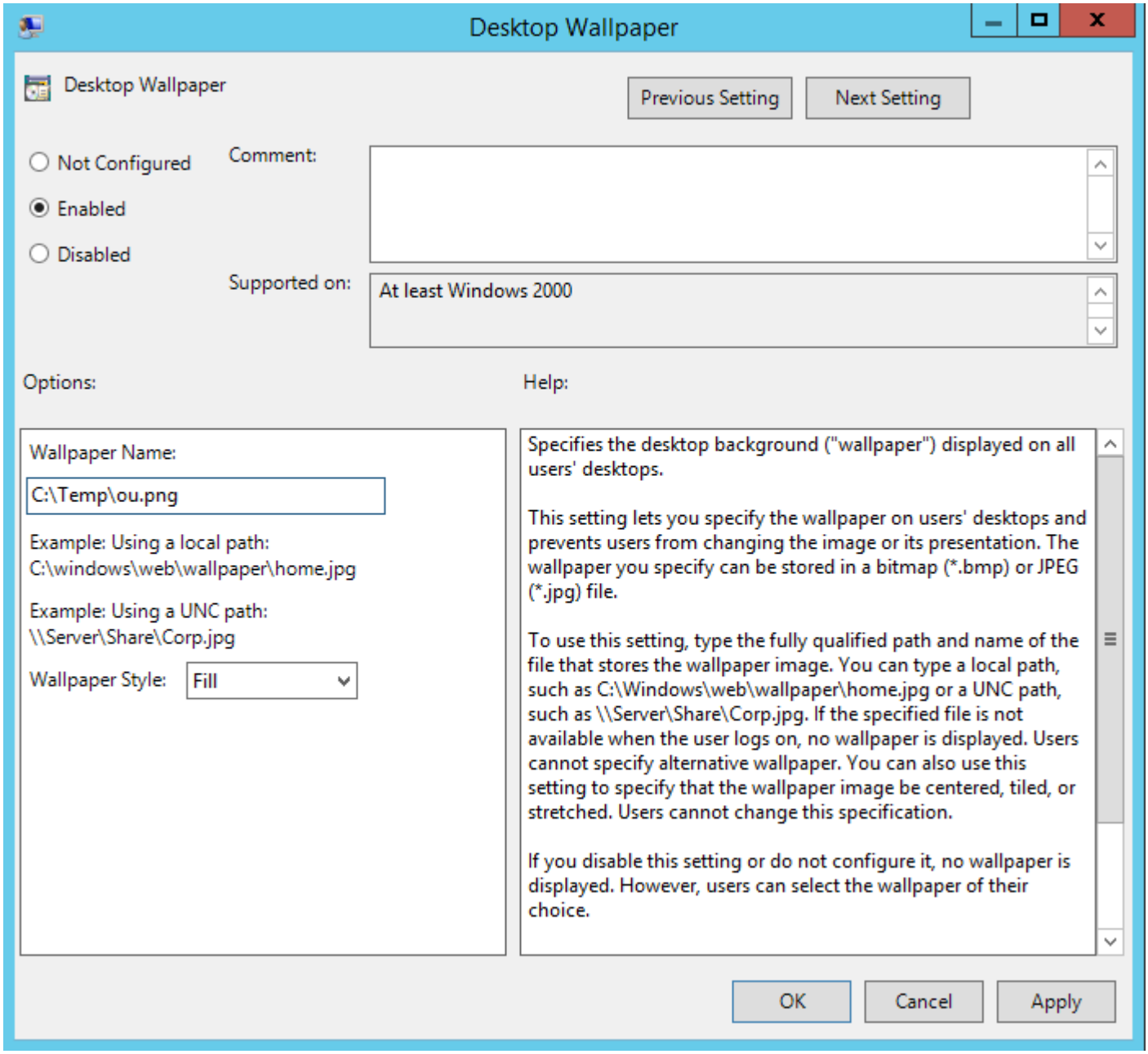



Еще раз заходим на WKS1 и удостоверяемся в том, что обои рабочего стола изменены и корзины не видно. Это значит, что доменные политики успешно применились и переопределили настройки, задаваемые локальными политиками.

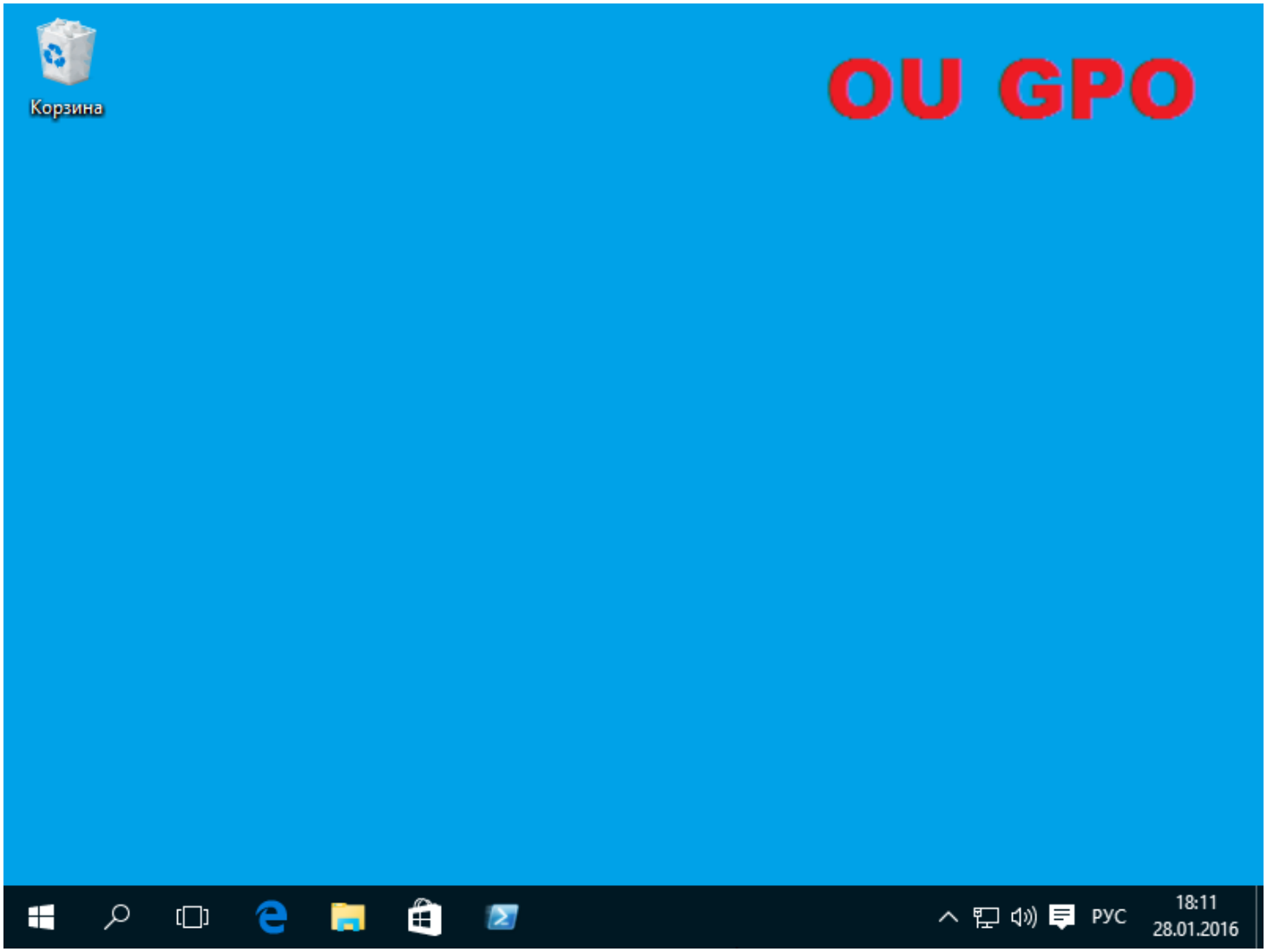
Ну и в качестве завершающего шага открываем на редактирование политику GPO4 и устанавливаем политику «Remove Recycle Bin icon from desktop» в положение Disabled.




А также меняем рисунок рабочего стола на изображение с именем ou.png.




Теперь, зайдя на WKS1 мы видим, что обои опять изменены и на рабочий стол вернулась корзина. Из этого следует, что доменная политика GPO2 переопределена политикой GPO4, назначенной на OU.



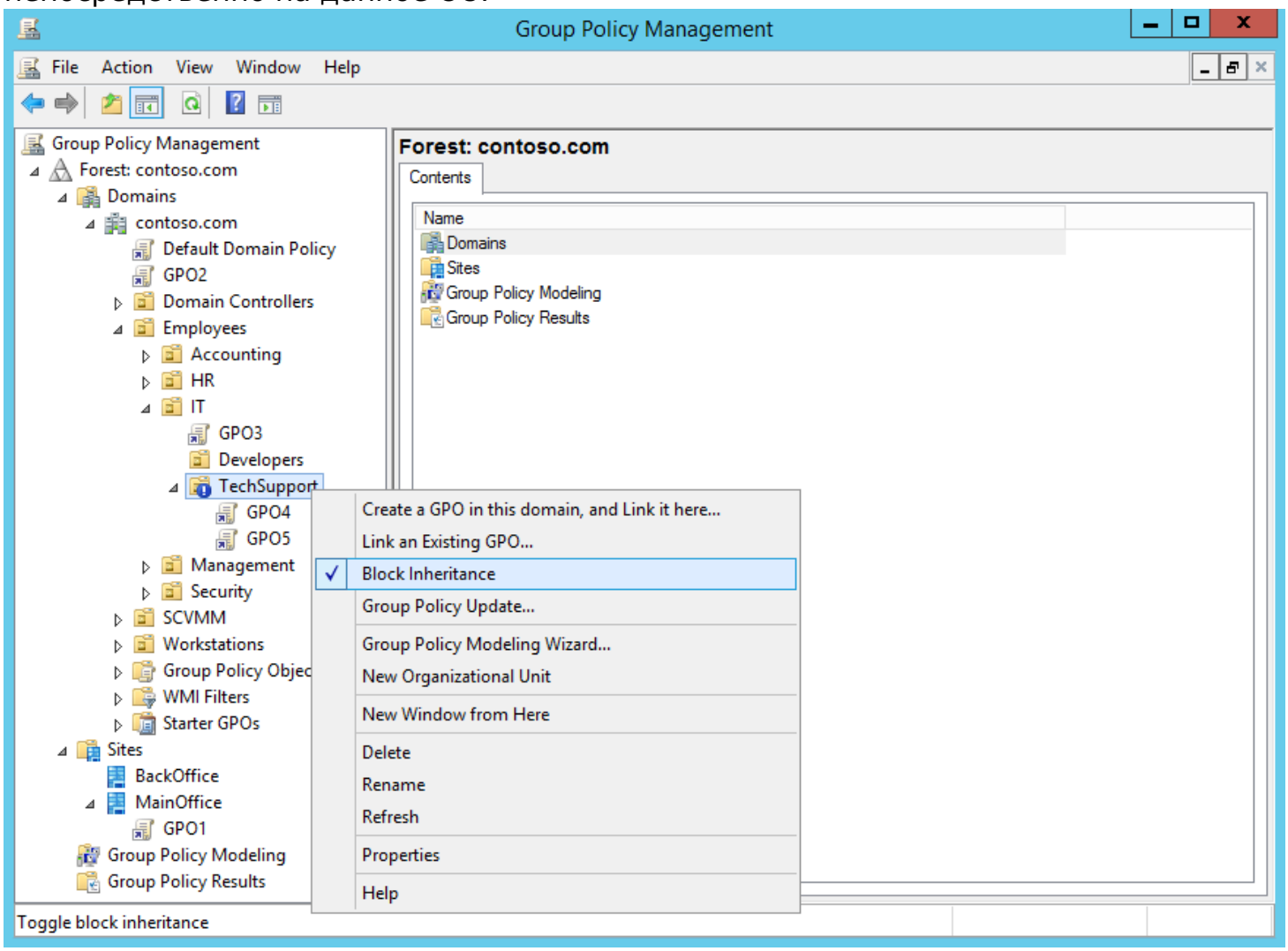

## Отключение наследования

Как я уже говорил, на все политики в домене распространяется наследование, т.е. политики, назначенные на родительский контейнер (домен или OU), последовательно применяются ко всем дочерним контейнерам. Это поведение по умолчанию, но при необходимости его можно изменить, отключив наследование для отдельно взятого OU.

Отключение наследования производится достаточно просто, надо только в оснастке «Group Policy Management» выбрать нужное OU, кликнуть на нем правой клавишей мыши и в контекстном меню отметить пункт «Block Inheritance». После этого для данного OU и его дочерних OU (при их наличии) отменяется воздействие всех вышестоящих политик.

**Примечание.** Политика Default Domain Policy содержит настройки, определяющие политику паролей и учетных записей в домене. Эти настройки не могут быть заблокированы.

В нашем примере отменим наследование для OU TechSupport, чтобы на него воздействовали только те политики, которые назначены непосредственно на данное OU.

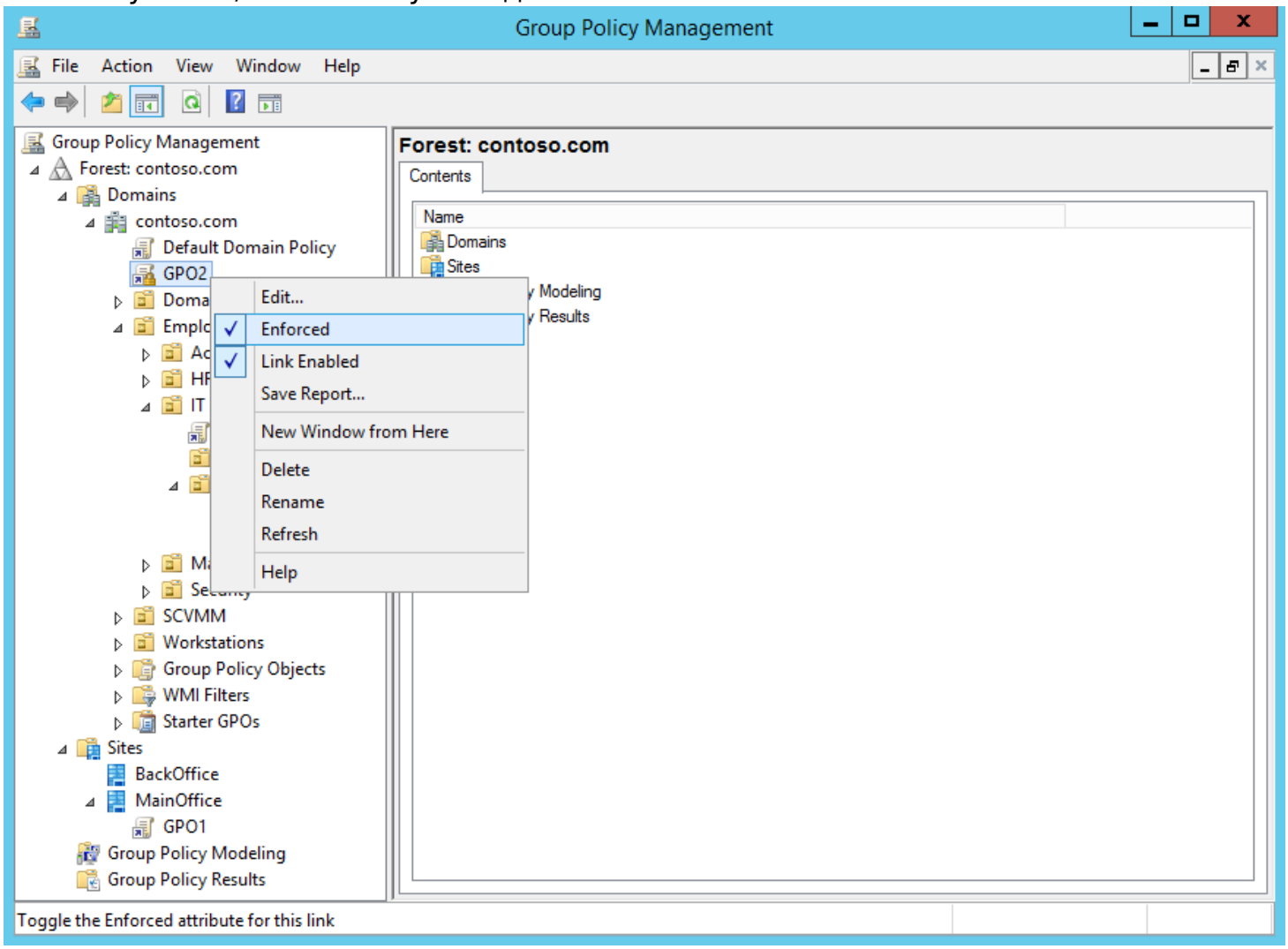



## Форсирование применения групповых политик

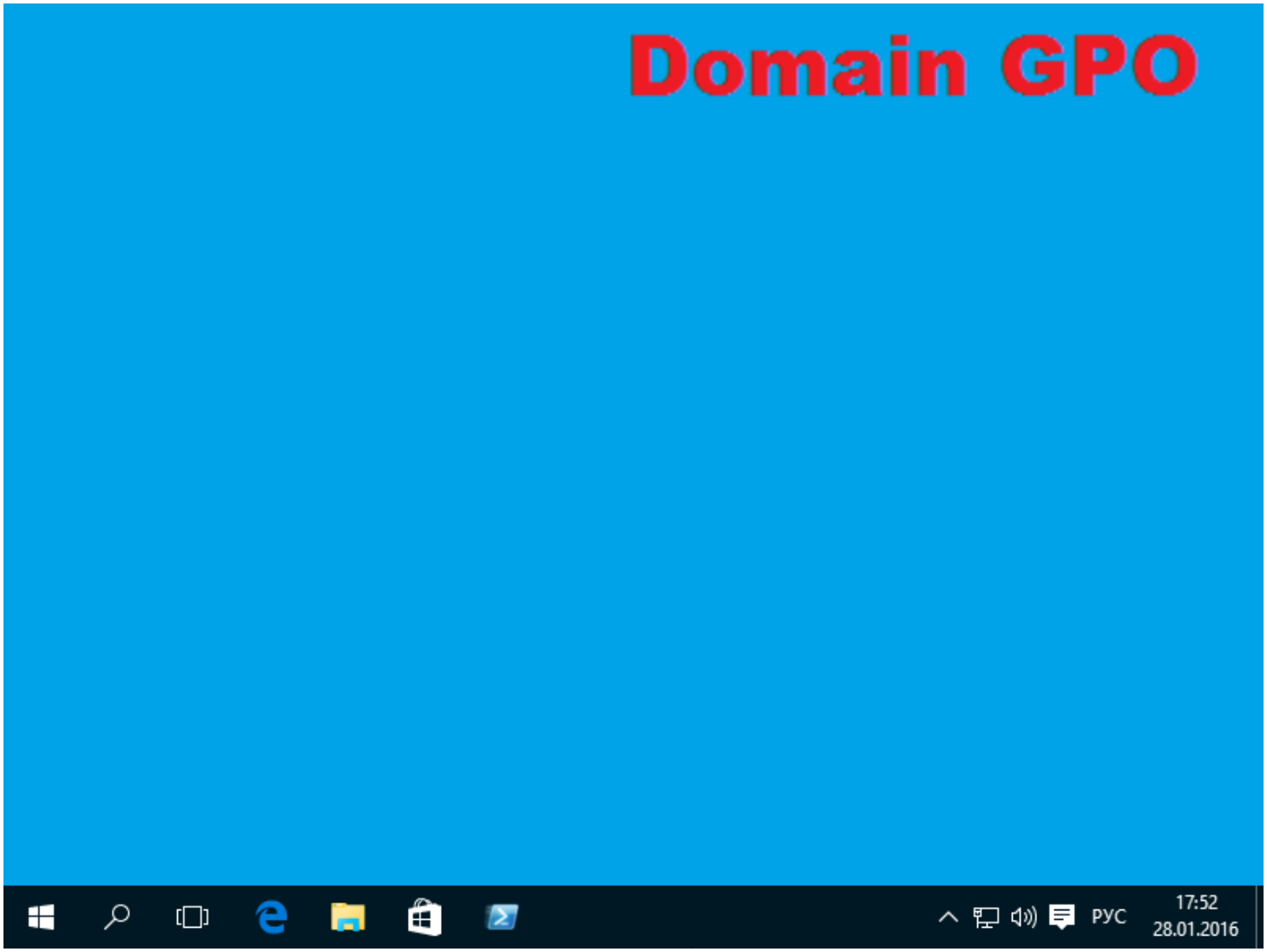
Форсирование применения групповых политик применяется тогда, когда данная политика должна отработать независимо от остальных политик. Если политика форсирована, то, вне зависимости от своей области действия она получает наивысший приоритет. Это значит, что ее настройки не могут быть переопределены нижестоящими политиками, а также на нее не действует отмена

наследования.

Чтобы форсировать политику, надо выбрать ее в оснастке управления групповыми политиками, кликнуть на ней правой клавишей мыши и в контекстном меню отметить пункт «Enforced». Для примера форсируем политику GPO2, назначенную на домен.




Затем зайдем на WKS1 еще раз и увидим знакомую картину. Как видите, политика GPO2 отработала не смотря на блокировку наследования и перебила настройки нижестоящей политики GPO4.




Дополнительная информация

Существует два способа применения объектов групповой политики на серверах служб терминалов, не оказывающих негативного влияния на другие серверы сети.

Способ 1

Объединение компьютеров сервера служб терминалов в собственное подразделение (OU). Такая конфигурация позволяет указать соответствующие настройки компьютеров в объектах групповой политики, которые применяются только к компьютерам сервера терминалов. Эта конфигурация не влияет на работу пользователей на рабочих станциях и других серверах и обеспечивает полный контроль над работой пользователей сервера терминалов. В подразделение не должны входить пользователи или другие компьютеры, чтобы обеспечить возможность тонкой настройки служб терминалов для администраторов домена.

Управление подразделением также можно делегировать подчиненным группам, например операторам сервера или отдельным пользователям.

Для создания нового подразделения для серверов служб терминалов выполните следующие действия.

1. Нажмите кнопку Пуск, выделите пункт Программы, затем пункт Администрирование и выберите команду **Пользователи и компьютеры Active Directory**.
2. Разверните левую область.
3. Щелкните пункт **domainname.xxx**.
4. В меню Действие выберите пункт Создать и щелкните Подразделение.
5. В поле Имя введите имя сервера служб терминалов.
6. Нажмите кнопку OK.

   Новое подразделение служб терминалов с объектами по умолчанию отобразится в списке в левой области. Серверы служб терминалов размещаются в подразделении «Компьютеры» или «Контроллеры домена».
7. Найдите и выделите серверы терминалов, откройте меню Действие и выберите команду Переместить.
8. В диалоговом окне Перемещение выделите новые серверы служб терминалов и нажмите кнопку OK.
9. Щелкните новое подразделение служб терминалов, чтобы убедиться в успешности перемещения.

Для создания объекта групповой политики служб терминалов выполните следующие действия.

1. Щелкните новое подразделение служб терминалов.
2. В меню Действие выберите команду Свойства.
3. Перейдите на вкладку Групповая политика.
4. Нажмите кнопку Создать, чтобы создать новый объект групповой политики.
5. Нажмите кнопку Правка, чтобы изменить групповую политику.

Способ 2

Использование возможности групповой политики, называемой замыканием на себя, для применения параметров GPO конфигурации пользователя к пользователям только при входе в систему серверов терминалов. Компьютеры подразделения,

содержащего серверы терминалов, для которых включен режим замыкания на себя объектов групповой политики, применяют параметры конфигурации пользователя из набора объектов групповой политики, которые применяются к этому подразделению. Кроме того, эти компьютеры применяют параметры конфигурации пользователя из объектов групповой политики, связанных с подразделением, содержащим учетную запись пользователя, или наследованных им.

Этот процесс описан в следующей статье базы знаний Майкрософт:

Режим замыкания на себя групповой политики (эта ссылка может указывать на содержимое полностью или частично на английском языке)

Реализация системных политик в службах терминалов Windows NT 4.0 также отличается от реализации на других серверах Windows NT и рассмотрена в следующей статье базы знаний Майкрософт:

Применение системных политик на сервере терминалов (эта ссылка может указывать на содержимое полностью или частично на английском языке)

По возможности службы терминалов следует устанавливать на рядовых серверах, а не на контроллерах домена, поскольку пользователям необходимо присвоить право Локальный вход в систему. Когда право Локальный вход в систему присваивается контроллерам домена, из-за общей базы данных Active Directory оно присваивается каждому контроллеру домена в домене. При установке служб терминалов в режиме серверного приложения право Локальный вход в систему в локальной политике безопасности присваивается рядовым серверам по умолчанию

## Список использованной литературы


1. https://windowsnotes.ru/activedirectory/primenenie-gruppovyx-politik-chast-1/
2. https://support.microsoft.com/ru-ru/help/260370/how-to-apply-group-policy-objects-to-terminal-services-servers
3. https://support.microsoft.com/ru-ru/help/260370/how-to-apply-group-policy-objects-to-terminal-services-servers