?????? ? GPO

????? ? ??????????? ? Active Directory

Права обычно назначаются пользователям или группам и касаются разрешений на доступ к объекту, такому как файл, в то время как привилегии предоставляют пользователю разрешение выполнять действие, такое как запуск программы, выключение системы, сброс паролей и т.д. Привилегии могут быть назначены индивидуально пользователям или предоставлены им через членство во встроенных или пользовательских группах. У Windows есть концепция, называемая Назначением Прав Пользователю, которая, хотя и называется правами, фактически представляет собой виды привилегий, предоставляемых пользователю.

?????????? ?????? ? Active Directory

AD содержит множество групп безопасности по умолчанию или встроенных групп, некоторые из которых предоставляют своим членам мощные права и привилегии, которые могут быть использованы злоумышленниками для повышения привилегий в пределах домена и, в конечном итоге, получения привилегий Domain Admin или SYSTEM на контроллере домена.

Ниже приведены некоторые из наиболее распространенных встроенных групп:

Название группы	Описание
Account Operators	Члены могут создавать и изменять большинство типов учетных записей, включая пользователей, локальные группы и глобальные группы, и могут входить локально на контроллеры домена. Не могут управлять учетной записью администратора и другими группами.
Administrators	Члены имеют полный и неограниченный доступ к компьютеру или всему домену, если они являются членами этой группы на контроллере домена.
Backup Operators	Члены могут резервировать и восстанавливать все файлы на компьютере, независимо от установленных на них разрешений. Могут также входить в систему и выключать компьютер.
DnsAdmins	Члены имеют доступ к сетевой информации DNS. Группа создается только при наличии или ранее установленной роли сервера DNS на контроллере домена.

Domain Admins	Члены имеют полный доступ к администрированию домена и являются членами группы локальных администраторов на всех компьютерах, присоединенных к домену.
Domain Computers	Все компьютеры, созданные в домене (за исключением контроллеров домена), добавляются в эту группу.
Domain Controllers	Содержит все контроллеры домена в домене. Новые контроллеры домена автоматически добавляются в эту группу.
Domain Guests	Включает в себя встроенную учетную запись Guest домена. Члены этой группы имеют профиль домена, созданный при входе на компьютер, присоединенный к домену, в качестве локального гостя.
Domain Users	Содержит все учетные записи пользователей в домене. Новая учетная запись пользователя в домене автоматически добавляется в эту группу.
Enterprise Admins	Членство в этой группе предоставляет полный доступ к конфигурации домена. Группа существует только в корневом домене леса AD. Члены группы имеют возможность вносить изменения, касающиеся всего леса.
Event Log Readers	Члены могут читать журналы событий на локальных компьютерах. Группа создается только при повышении уровня хоста до контроллера домена.
Group Policy Creator Owners	Члены создают, редактируют или удаляют объекты групповой политики в домене.
Hyper-V Administrators	Члены имеют полный и неограниченный доступ ко всем функциям Hyper-V. Если в домене есть виртуальные контроллеры домена, любые администраторы виртуализации, такие как члены Hyper-V Administrators, должны рассматриваться как Domain Admins.
IIS_IUSRS	Это встроенная группа, используемая службой Internet Information Services (IIS) начиная с версии IIS 7.0.
Pre–Windows 2000 Compatible Access	Группа существует для обеспечения обратной совместимости с компьютерами, работающими под управлением Windows NT 4.0 и более ранних версий. Членство в этой группе часто представляет собой остаточную легаси-конфигурацию.
Print Operators	Члены могут управлять, создавать, делиться и удалять принтеры, подключенные к контроллерам домена, а также любые объекты принтеров в AD. Могут входить локально на контроллеры домена и использоваться для загрузки вредоносного драйвера принтера и повышения привилегий в домене.

Protected Users	Члены этой группы обеспечиваются дополнительной защитой от кражи учетных данных и тактик, таких как злоупотребление Kerberos.
Read-only Domain Controllers	Содержит все контроллеры домена с привилегиями только для чтения в домене.
Remote Desktop Users	Эта группа используется для предоставления пользователям и группам разрешения на подключение к хосту через удаленный рабочий стол (RDP). Эту группу нельзя переименовать, удалить или переместить.
Remote Management Users	Эта группа может использоваться для предоставления пользователям удаленного доступа к компьютерам через Windows Remote Management (WinRM).
Schema Admins	Члены могут модифицировать схему Active Directory, которая определяет все объекты в AD. Группа существует только в корневом домене леса AD. Администратор корневого домена леса является единственным членом этой группы по умолчанию.
Server Operators	Эта группа существует только на контроллерах домена. Члены могут изменять службы, получать доступ к SMB-ресурсам и выполнять резервное копирование файлов на контроллерах домена. По умолчанию в этой группе нет членов.

?????????? ???? ???????????

В зависимости от групп, в которых они состоят, и других факторов, таких как привилегии, назначаемые администраторами через Политику Группы (GPO), у пользователей могут быть разные права на свои учетные записи. В статье Microsoft о Назначении Прав Пользователю предоставляется подробное объяснение каждого права, которое может быть установлено в Windows. Некоторые могут привести к непреднамеренным последствиям, таким как повышение привилегий или доступ к чувствительным файлам. Допустим, мы получаем права на запись в объект Групповой политики (GPO), примененной к подразделению (OU) с одним или несколькими пользователями, которыми мы управляем. В этом случае мы можем использовать инструменты, такие как SharpGPOAbuse, чтобы назначить целевые права пользователю. Таким образом, мы можем расширить свой доступ в домен, выполняя различные действия с этими новыми правами. Например:

Привилегия	**Описание**
SeRemoteInteractiveLogonRight	Может предоставить целевой учетной записи право входа на хост через удаленный рабочий стол (RDP), что потенциально может быть использовано для получения чувствительных данных или повышения привилегий

SeBackupPrivilege	Предоставляет пользователю возможность создавать резервные копии системы и может быть использована для получения копий чувствительных системных файлов, которые могут быть использованы для извлечения паролей, таких как файлы реестра SAM и SYSTEM и файл базы данных Active Directory NTDS.dit.
SeDebugPrivilege	Позволяет пользователю отлаживать и настраивать память процесса. С этой привилегией атакующие могут использовать инструменты, такие как Mimikatz, для чтения области памяти процесса Local System Authority (LSASS) и получения любых учетных данных, хранящихся в памяти.
SeImpersonatePrivilege	Позволяет поддельно представлять токен привилегированной учетной записи, такой как NT AUTHORITY\SYSTEM. Это может быть использовано с инструментами, такими как JuicyPotato, RogueWinRM, PrintSpoofer и др. для повышения привилегий на целевой системе.
SeLoadDriverPrivilege	Пользователь с этой привилегией может загружать и выгружать драйверы устройств, которые могут быть использованы для повышения привилегий или компрометации системы.
SeTakeOwnershipPrivilege	Позволяет процессу завладеть объектом. На самом простом уровне мы можем использовать эту привилегию, чтобы получить доступ к общей папке или файлу на общей папке, к которым у нас иначе не было бы доступа.

???????? ??????????? ????????????

После входа на хост, введение команды `whoami /priv` предоставит нам список всех назначенных пользовательских прав. Некоторые права доступны только для административных пользователей и могут быть перечислены/использованы только при выполнении повышенной сессии CMD или PowerShell. Понятия повышенных прав и Контроля учетных записей пользователя (User Account Control, UAC) являются функциями безопасности, введенными в Windows Vista, которые по умолчанию ограничивают приложения в выполнении с полными разрешениями, если это абсолютно необходимо. Если мы сравним и контрастируем права, доступные нам в качестве администратора в консоли без повышения привилегий и в консоли с повышенными привилегиями, мы увидим, что они существенно отличаются.

????????? ????????

Group Policy (Групповая политика) — это функция Windows, предоставляющая администраторам широкий набор настроек, которые могут применяться как к учетным записям пользователей, так и к компьютерам в среде Windows. У каждого хоста Windows есть редактор локальной групповой политики для управления локальными настройками.

С точки зрения безопасности использование групповых политик — это один из лучших способов влияния на уровень безопасности организации. Active Directory, безусловно, не обладает достаточной безопасностью "из коробки", и групповые политики являются ключевой частью стратегии защиты.

??????? ????????? ???????? (GPO)

Объект групповой политики (Group Policy Objects) — это виртуальная коллекция параметров политики, которые можно применять к пользователям или компьютерам. GPO включают в себя такие политики, как тайм-аут блокировки экрана, отключение USB-портов, применение политики паролей собственного домена, установку программного обеспечения, управление приложениями, настройку параметров удаленного доступа и многое другое. Каждый объект групповой политики имеет уникальное имя и уникальный идентификатор (GUID). Их можно связать с конкретным доменом или сайтом. Один объект групповой политики может быть связан с несколькими контейнерами, и к любому контейнеру может быть применено несколько объектов групповой политики. Их можно применять к отдельным пользователям, хостам или группам путем применения непосредственно к подразделению. Каждый объект групповой политики содержит один или несколько параметров групповой политики, которые могут применяться на уровне локального компьютера или в контексте Active Directory.

??????? ???????? ????????? ????????

Вот некоторые примеры того, что мы можем сделать с объектами групповой политики:

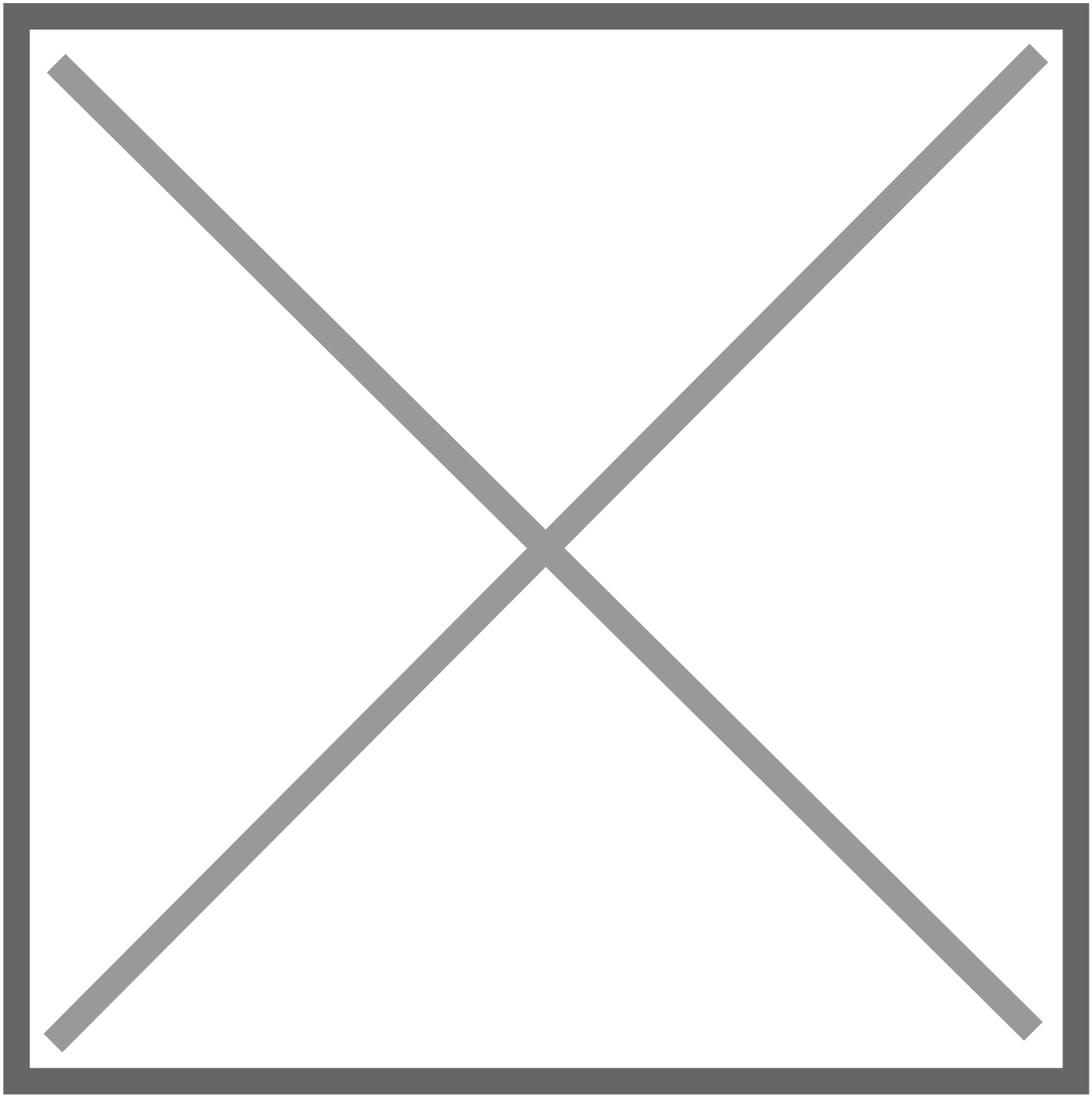
- Установка различных политик паролей для учетных записей служб, учетных записей администратора и обычных учетных записей пользователей с использованием отдельных объектов групповой политики.
- Запрет на использование съемных носителей (например, USB-устройств)
- Включение защиты заставки с помощью пароля
- Ограничение доступа к приложениям, которые могут не понадобиться обычному пользователю, например cmd.exe и PowerShell.
- Обеспечение соблюдения политик аудита и ведения журналов
- Блокировка пользователям запуска определенных типов программ и скриптов
- Развертывание программного обеспечения в домене
- Блокировка установки не одобренного программного обеспечения
- Отображение баннера входа в систему каждый раз, когда пользователь входит в систему
- Запрет использования LM-хеша в домене

- Запуск сценариев при запуске/выключении компьютеров или когда пользователь входит в систему или выходит из нее.

Давайте возьмем в качестве примера реализацию Active Directory в Windows Server 2008 по умолчанию, сложность пароля применяется по умолчанию. Требования к сложности пароля следующие:

- Пароли должны быть длиной не менее 7 символов.
- Пароли должны содержать символы как минимум трех из следующих четырех категорий:
  1. Символы верхнего регистра (A-Z)
  2. Символы нижнего регистра (a-z)
  3. Числа (0-9)
  4. Специальные символы (например, !@#$%^&*()_+|~-=`{}[]:";'<>?,./)

Это всего лишь несколько примеров того, что можно сделать с помощью групповой политики. В объекте групповой политики можно применять сотни настроек, которые могут быть очень детализированными. Например, ниже приведены некоторые параметры, которые мы можем установить для сеансов удаленного рабочего стола:



Настройки объекта групповой политики обрабатываются с использованием иерархической структуры AD и применяются с использованием правила порядка старшинства, как показано в таблице ниже:

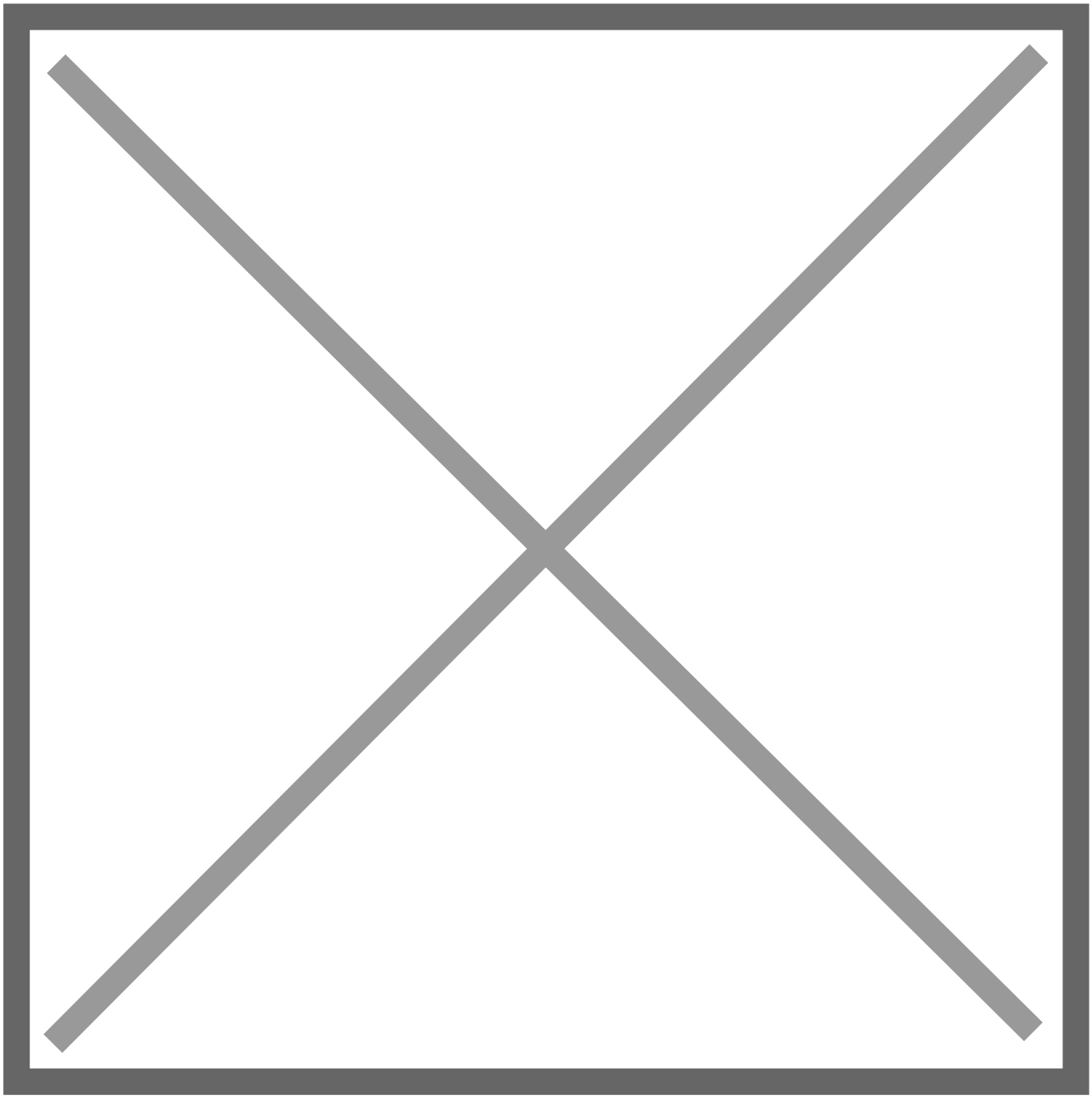
Уровень	Описание
Local Group Policy	Политики определяются непосредственно на хосте локально за пределами домена. Любая настройка здесь будет перезаписана, если аналогичная настройка определена на более высоком уровне.

Уровень	Описание
Site Policy	Любые политики, специфичные для физической локации, в которой находится хост. Организации могут охватывать большие кампусы и даже страны, поэтому само собой разумеется, что у локации могут быть свои собственные политики, которые могут отличаться от остальной части организации (например, для центрального офиса и филиалов).
Domain-wide Policy	Любые настройки, которые применяются ко всему домену в целом. Например, установка уровня сложности политики паролей, настройка фона рабочего стола для всех пользователей и установка баннера «Уведомление об использовании и согласие на мониторинг» на экране входа в систему.
Organisational Unit (Подразделение, OU)	Эти параметры будут влиять на пользователей и компьютеры, принадлежащие определенным подразделениям. Например, доступ к определенному общему диску, доступ к которому может получить только отдел кадров, доступ к определенным ресурсам, таким как принтеры, или возможность ИТ-администраторам использовать PowerShell и командную строку.
Любые политики подразделения (OU), вложенные в другие подразделения (OU)	Включают в себя специальные разрешения для объектов внутри вложенных подразделений. Например, предоставление аналитикам безопасности определенного набора параметров политики Applocker, которые отличаются от стандартных параметров IT Applocker.

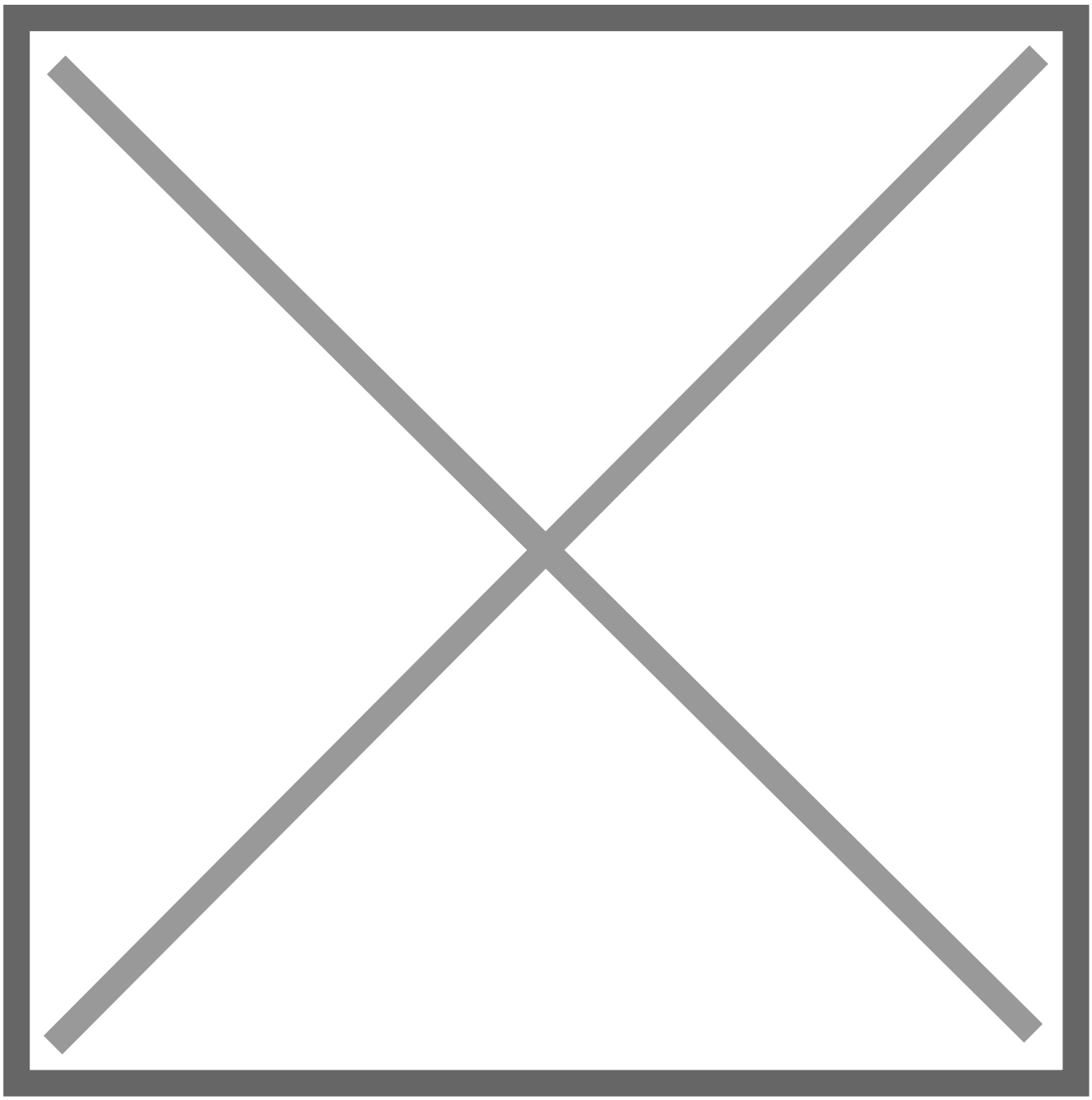
На изображении ниже показан пример нескольких объектов групповой политики, связанных с подразделением Corp. Если с подразделением связано более одного объекта групповой политики, они обрабатываются на основе порядка связывания (Link Order). Объект групповой политики с наименьшим порядком обрабатывается последним, либо объект групповой политики с порядком 1 имеет наивысший приоритет, затем 2, 3 и т. д. Таким образом, в нашем примере выше объект групповой политики Disallow LM Hash будет иметь приоритет над объектами групповой политики Block Removable Media и Disable Guest Account, то есть он будет обработан первым.

Можно указать параметр «Принудительно», чтобы применить настройки в конкретном объекте групповой политики. Если этот параметр установлен, параметры политики в объектах групповой политики, связанных с подразделениями нижнего уровня, **не могут** переопределить (override) эти параметры. Если объект групповой политики установлен на уровне домена с выбранным параметром «Принудительно», параметры, содержащиеся в этом объекте групповой политики, будут применены ко всем подразделениям в домене и не могут быть переопределены политиками подразделений более низкого уровня. Раньше этот параметр назывался «No Override» и устанавливался для соответствующего контейнера в разделе «Пользователи и компьютеры Active Directory» (Users and Computers). Ниже мы можем увидеть пример принудительного объекта групповой политики, где объект

групповой политики Logon Banner имеет приоритет над объектами групповой политики, связанными с нижними подразделениями, и поэтому не будет переопределен.

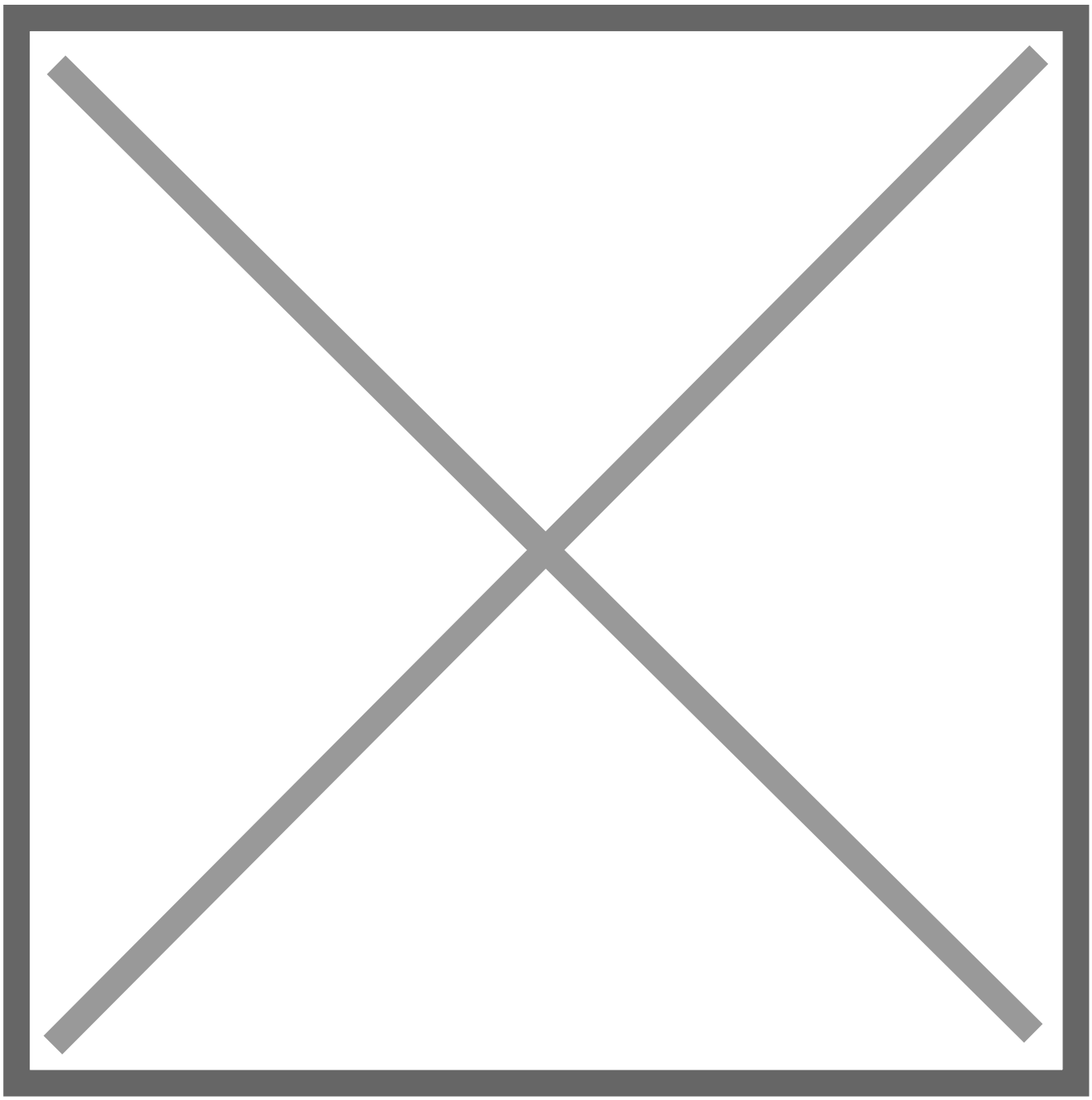


Принудительный приоритет политики объекта групповой политики:

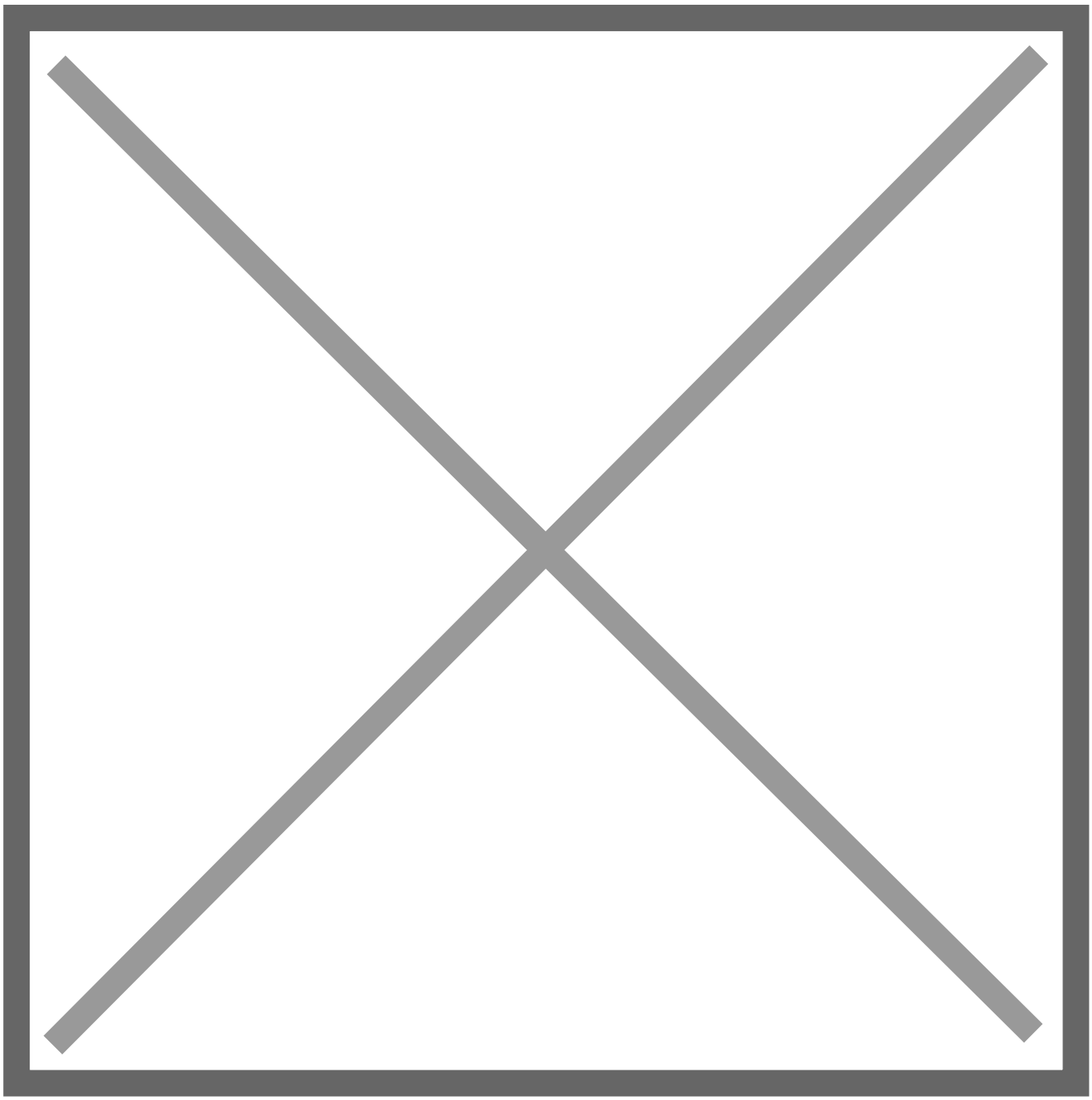


Независимо от того, для какого объекта групповой политики установлено принудительное применение, если применяется объект групповой политики доменной политики по умолчанию, он будет иметь приоритет над всеми объектами групповой политики на всех уровнях.

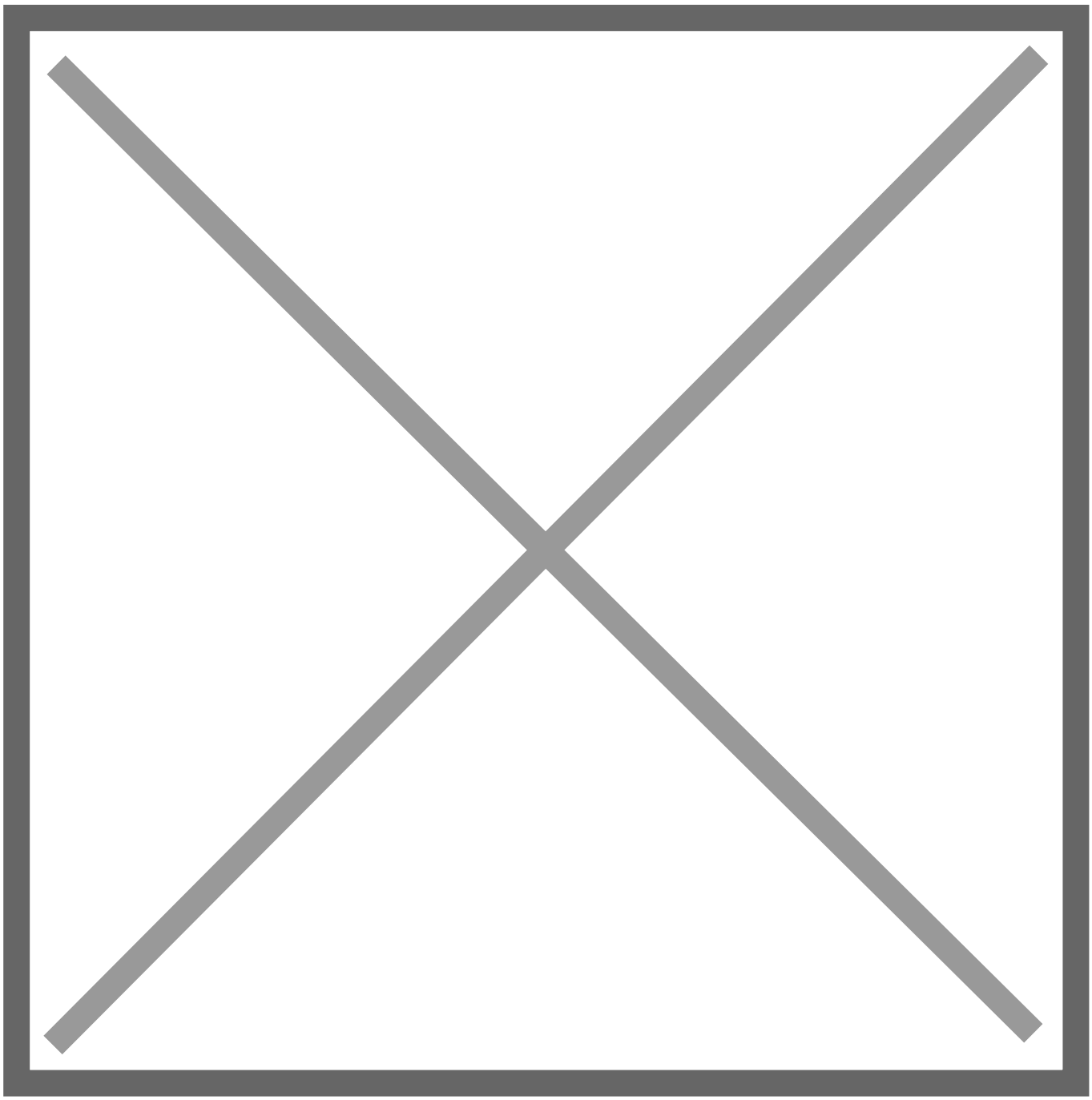
?????????????? ???????? ?????? ?? ?????????



Также можно установить параметр Block inheritance (блокировать наследование) для подразделения. Если это указано для конкретного подразделения, то политики более высокого уровня (например, на уровне домена) не будут применяться к этому подразделению. Если установлены оба параметра, параметр No Override имеет приоритет над параметром Block inheritance. Например, подразделение Computers наследует объекты групповой политики, установленные в подразделении Corp, как показано на рисунке ниже:



Если выбран параметр Block inheritance, мы увидим, что три объекта групповой политики, примененные выше к подразделению Corp, больше не применяются к подразделению Computers:



?????????? GPO ? ????????? ??????????????????

GPO (Group Policy Object) — это мощный инструмент управления настройками безопасности в сетевых средах, который позволяет администраторам контролировать рабочие станции и серверы в рамках целой организации. Для членов Blue Team знание GPO особенно важно, так как это позволяет повысить уровень безопасности IT-инфраструктуры, применяя единую политику конфигураций, безопасности и управления.

???????? GPO ? ??????????? ????????????? ??????? ??????

GPO — это набор настроек, который создается в административном шаблоне и применяется к объектам Active Directory, таким как пользователи, группы, компьютеры и папки. Эти политики позволяют автоматизировать и стандартизировать конфигурационные и безопасностные настройки, управлять установкой программного обеспечения, обновлением паролей, ограничениями доступа и другими важными аспектами IT-систем.

??????????? Group Policy Objects ? Windows

????????? GPO (Local Group Policy Objects)

Локальные GPO применяются к конкретному компьютеру и хранятся локально на этом компьютере. Они могут быть настроены непосредственно на самом компьютере без необходимости подключения к сети или домену. Обычно они используются для установки базовых настроек безопасности или конфигурации на отдельных компьютерах, например, для ограничения доступа к определенным ресурсам или приложениям. Их можно настроить через локальный Group Policy Editor (gpedit.msc).

??????? GPO (Network Group Policy Objects)

Сетевые GPO хранятся на контроллерах домена и применяются к объектам в Active Directory, таким как пользователи, компьютеры или группы. Они позволяют централизованно управлять настройками безопасности и конфигурацией для всех объектов в сети, которые являются частью домена. Сетевые GPO могут быть применены к организационным единицам (Organizational Units, OU), группам или пользователям. Они могут настраиваться через Group Policy Management Console (GPMC), доступный на контроллерах домена. Применение сетевых GPO особенно полезно в средних и крупных сетях, где требуется централизованное управление настройками и безопасностью на всех устройствах и для всех пользователей.

Иерархия GPO обычно основывается на принципе "наследования". Это означает, что настройки из сетевых GPO могут наследоваться от более общих к более конкретным уровням Active Directory, таким как домен, организационная единица (OU), группа и пользователь. Локальные GPO имеют более высокий приоритет применения, чем сетевые GPO, поскольку они применяются непосредственно к конкретному компьютеру.

????? GPO ? Group Policy Management Console (GPMC)

GPO, GPMC ? RSoP

- **GPO** (Group Policy Object) — это инструменты для управления настройками безопасности и конфигурации в среде Windows.
- **GPMC** (Group Policy Management Console) — централизованный интерфейс для работы с GPO.
- **RSoP** (Resultant Set of Policy) — показывает результирующий набор политик, применяемых к конкретному пользователю или компьютеру.

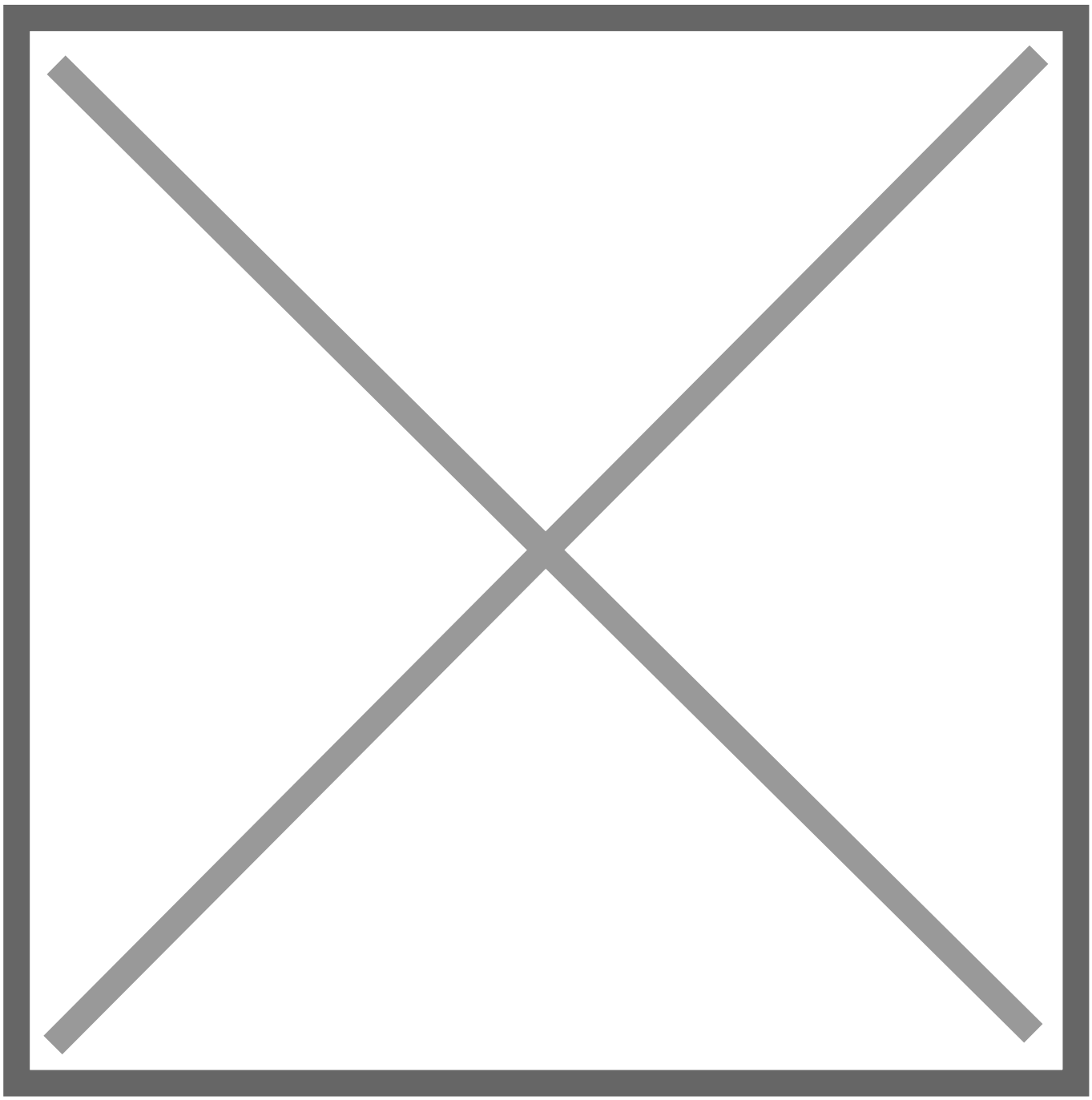
???????? ? ??????????? GPO ? ????????????????? Group Policy Management Console (GPMC)

GPMC предлагает графический интерфейс для создания, редактирования и удаления GPO. Этот инструмент интегрируется с Active Directory и позволяет администраторам назначать политики на уровне доменов, сайтов и отдельных организационных единиц.

???????? GPO ????? GPMC

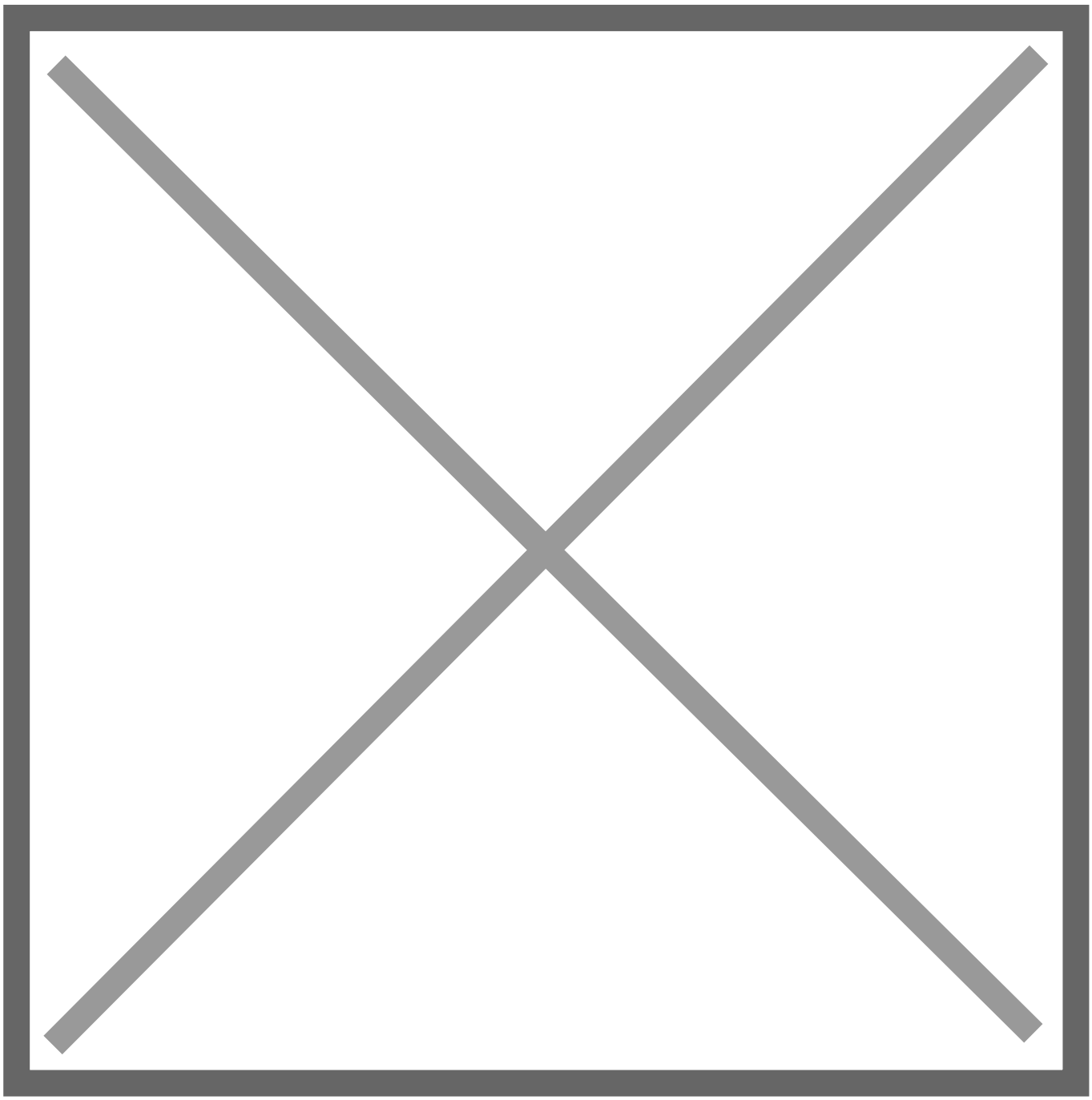
Создание нового GPO в GPMC просто:

- нажмите правой кнопкой мыши на соответствующей организационной единице;
- выберите "Создать GPO в этом домене и связать его здесь";
- задайте соответствующие настройки.



?????????????? GPO

Для редактирования существующего GPO, щелкните по нему правой кнопкой мыши и выберите "Изменить", после чего откроется редактор политик, где можно настроить необходимые параметры в разделах "Конфигурация компьютера" и "Конфигурация пользователя".



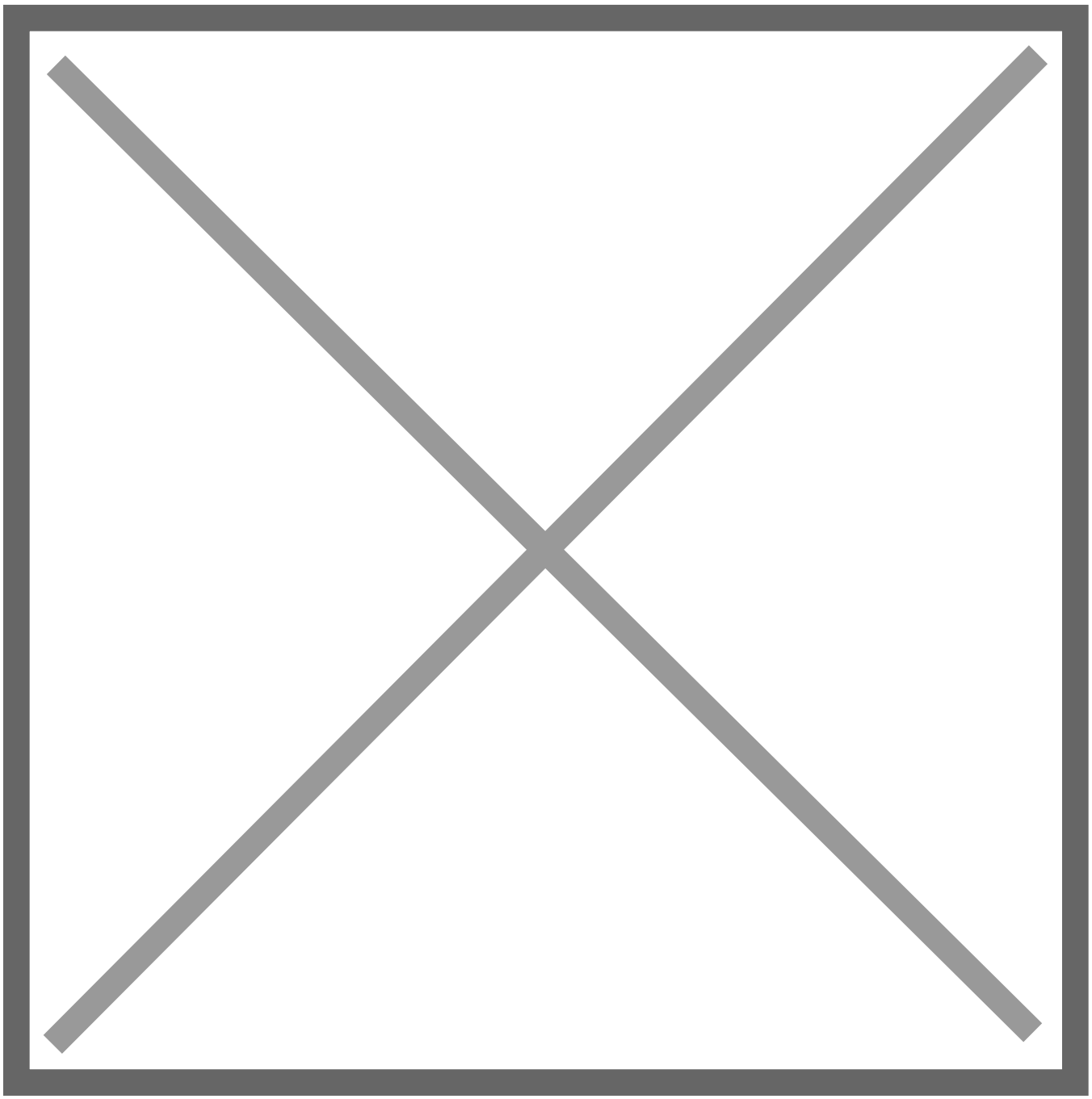
Управление GPO

С помощью GPMC можно также управлять связями GPO, задавать фильтры безопасности для контроля применения политик к определенным пользователям или группам, а также использовать WMI-фильтры для более гранулированного применения политик на основе атрибутов компьютера.

?????????? ????????? ??? AD ? Windows Server

В предыдущих темах мы рассматривали CIS Benchmarks — эти рекомендации также существуют и для GPO. В этом разделе мы рассмотрим, как реализовать набор сборки CIS L1 на домене Server 2019.

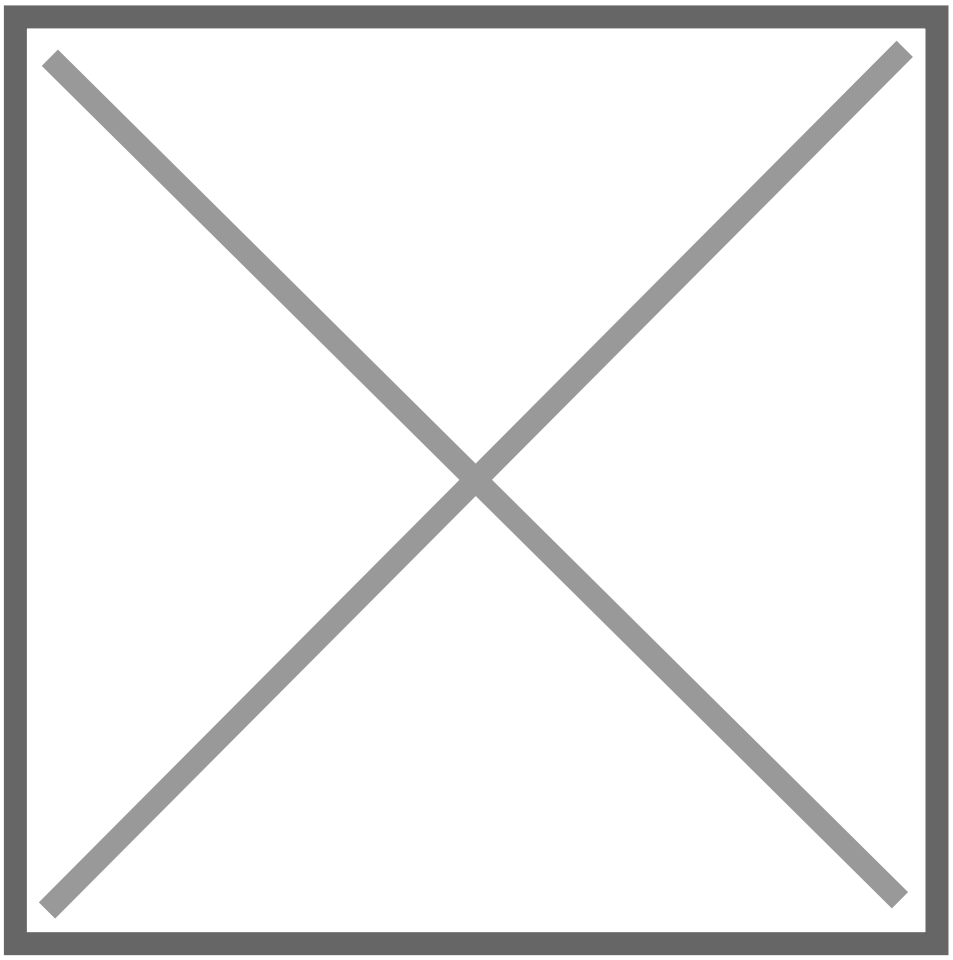
CIS Benchmark для GPO включает в себя матрицу:



Мы будем использовать 3 GPO:

- USER L1 - пользователи первого уровня;
- DC-L1 - контроллер домена первого уровня;
- DC-L1 Services - сервисы контроллера домена первого уровня.

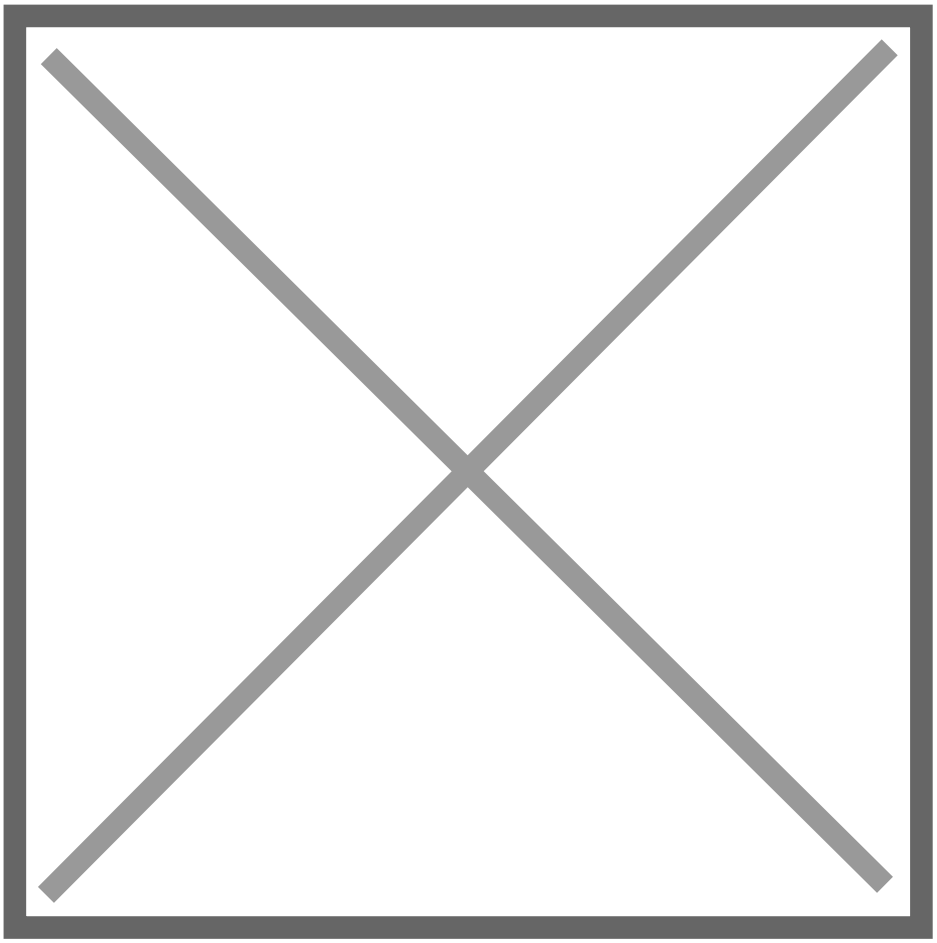
В Server 2019 откройте консоль управления групповыми политиками (GPMC) и создайте новый объект групповой политики. Дадим ему то же самое имя, что и стандарт CIS:



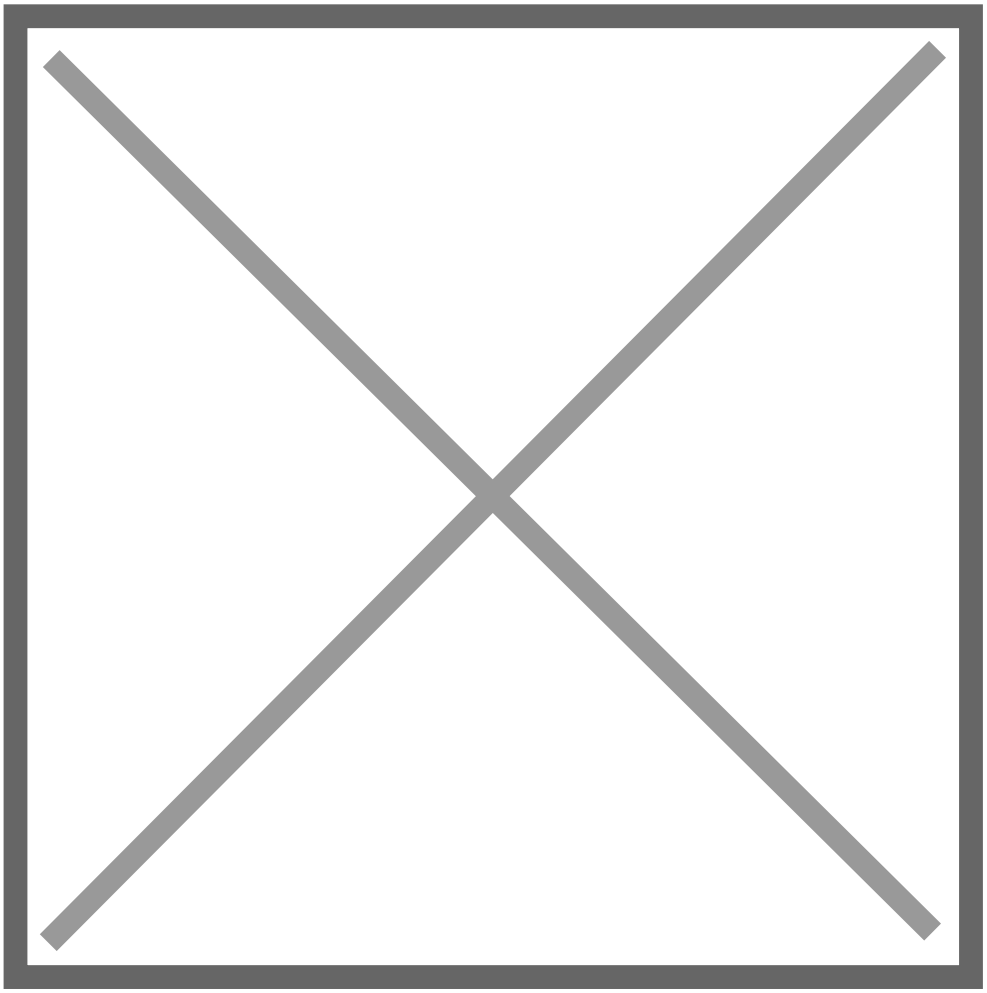
Затем щелкните правой кнопкой мыши на созданной GPO и выберите "Import Settings" (Импортировать настройки), это запустит мастер импорта настроек.

Вас попросят создать резервную копию существующей GPO, это можно пропустить, поскольку это новая GPO. Но если бы это была существующая GPO, рекомендуется выполнить резервное копирование, так как все настройки будут перезаписаны, и резервную копию можно будет использовать в случае, если нужно будет выполнить откат настроек.

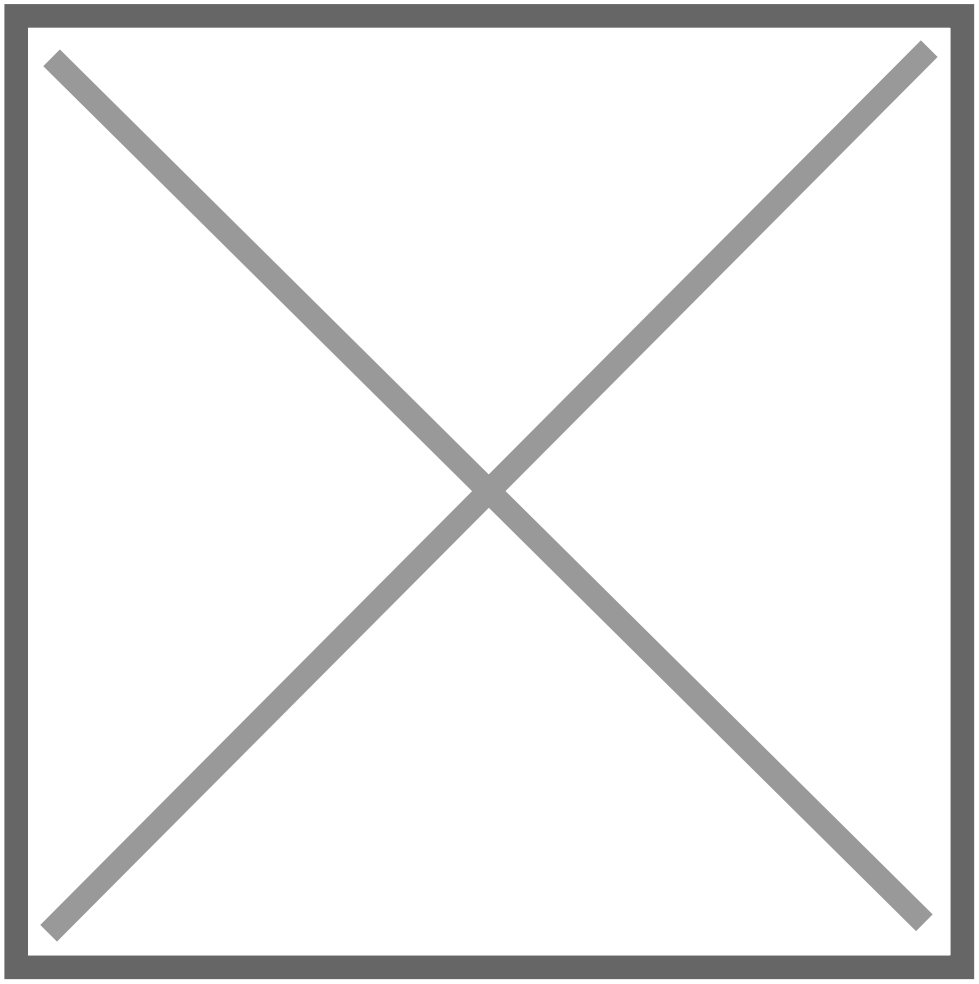
Затем вам будет предложено указать путь к папке "резервной копии" для импорта настроек. На первый взгляд этот шаг может показаться немного запутанным, так как предыдущий экран был о резервных копиях. На самом деле это путь к GPO комплекту сборки CIS, который нам нужно указать для импорта в нашу новую GPO. Ниже мы выбираем путь к нашей папке USER-L1:

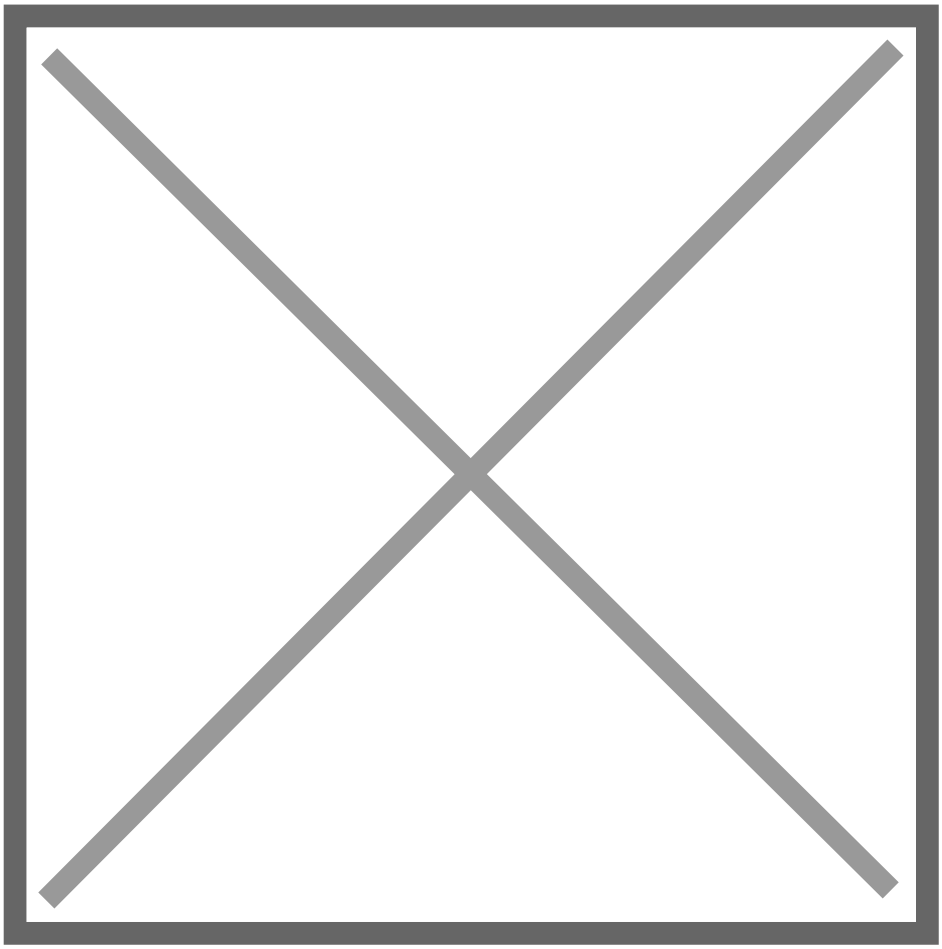


На следующем экране вы получите подтверждение найденной GPO:



Подтвердите настройки:

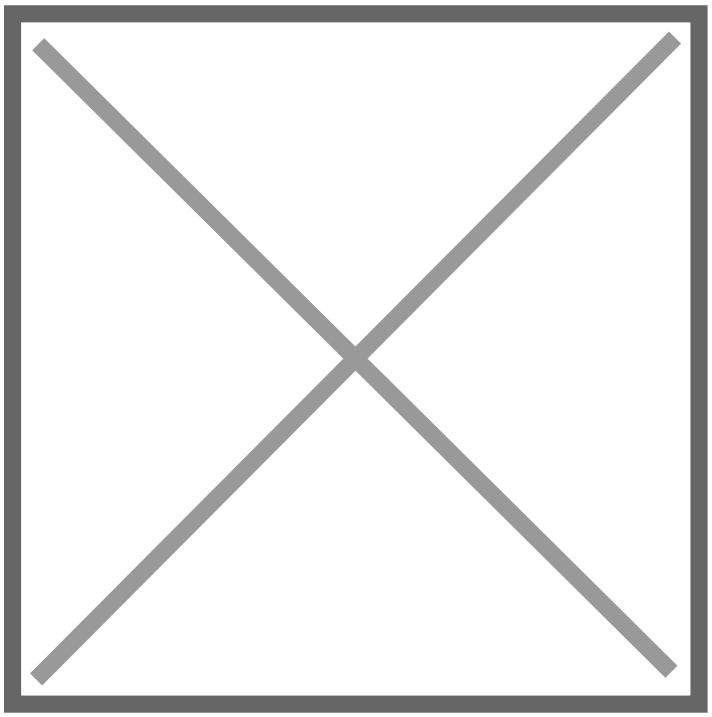




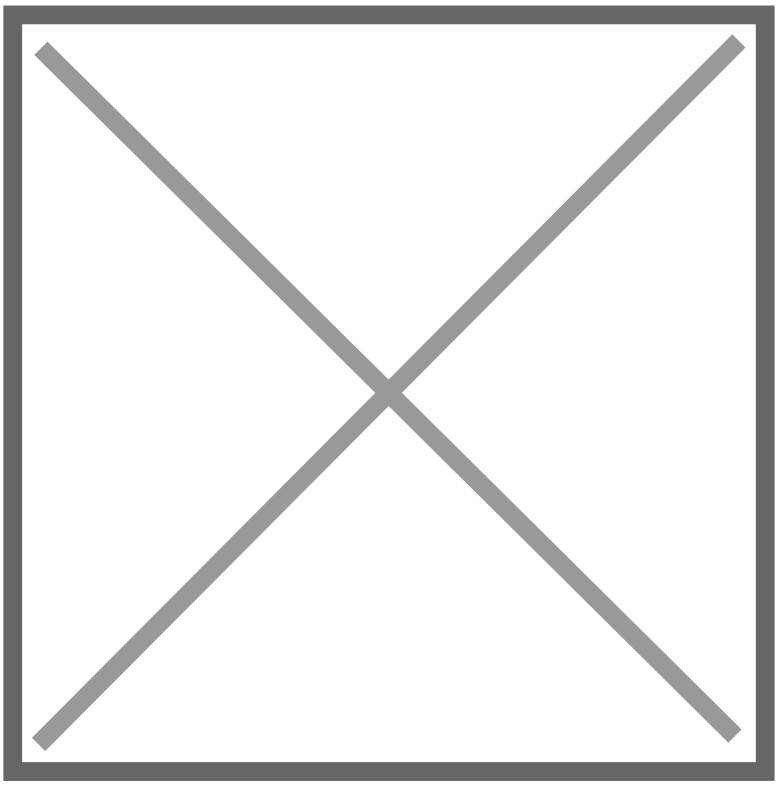
?????????? GPO

Сейчас импортированные GPO не связаны с какими-либо организационными единицами (OU) в Active Directory и не активны.

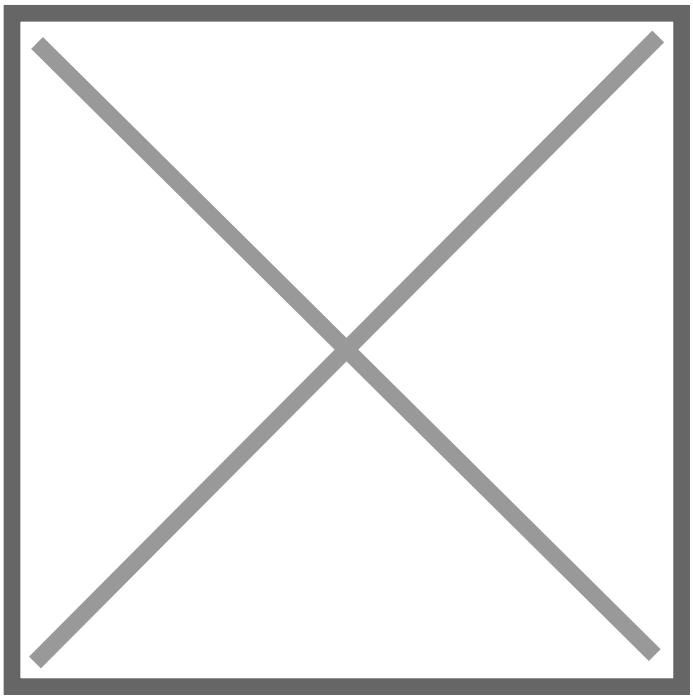
Для связывания GPO нажмите правой кнопкой мыши на OU домена (или на той OU, с которой вы хотите связать GPO) и выберите "Link an existing GPO" (Связать существующий GPO).



Выберите GPO:



Эти GPO затем появятся под выбранной вами ранее OU:



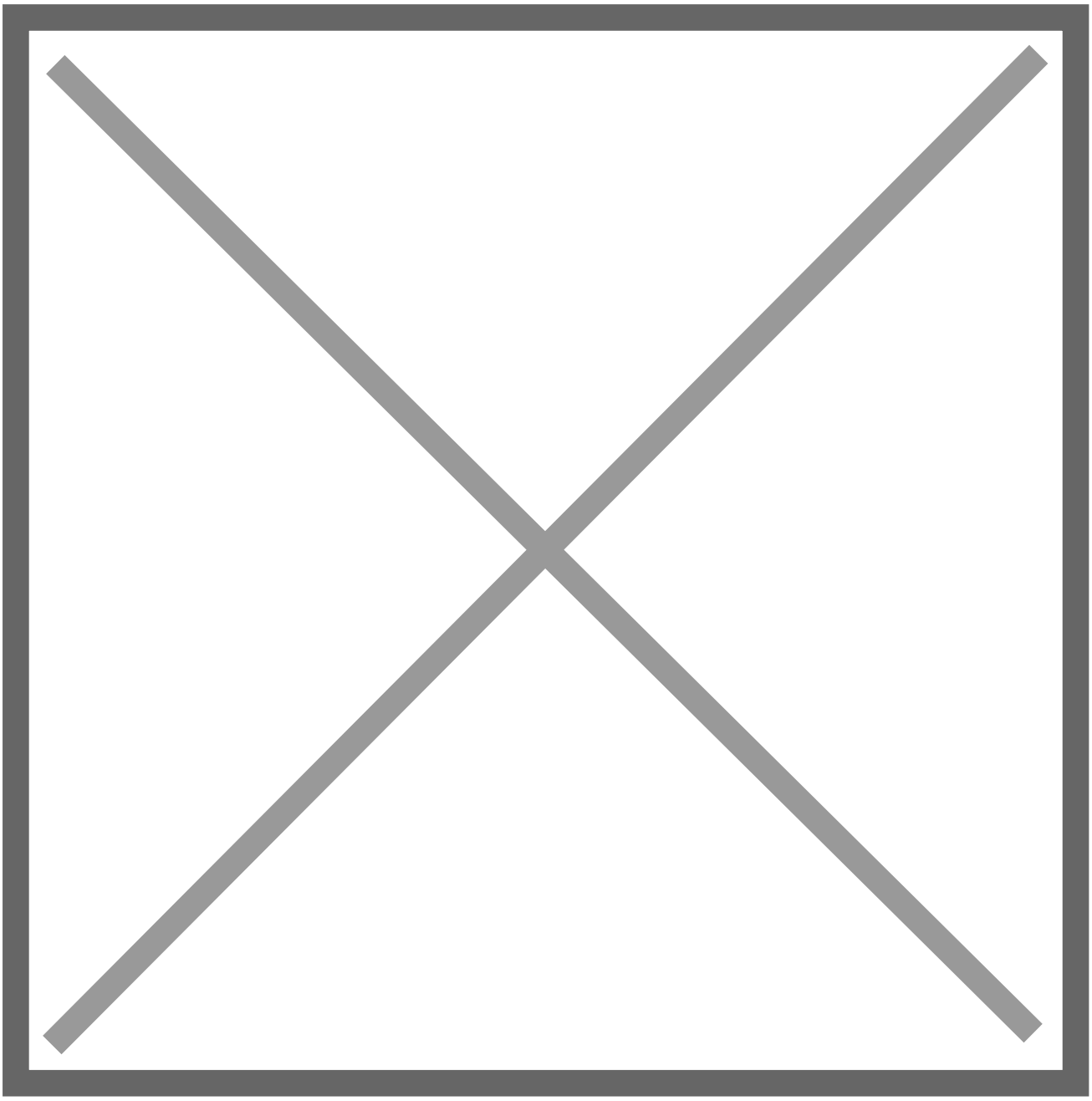
Теперь GPO активны и должны распространяться на все системы в вашем домене Active Directory.

??????????

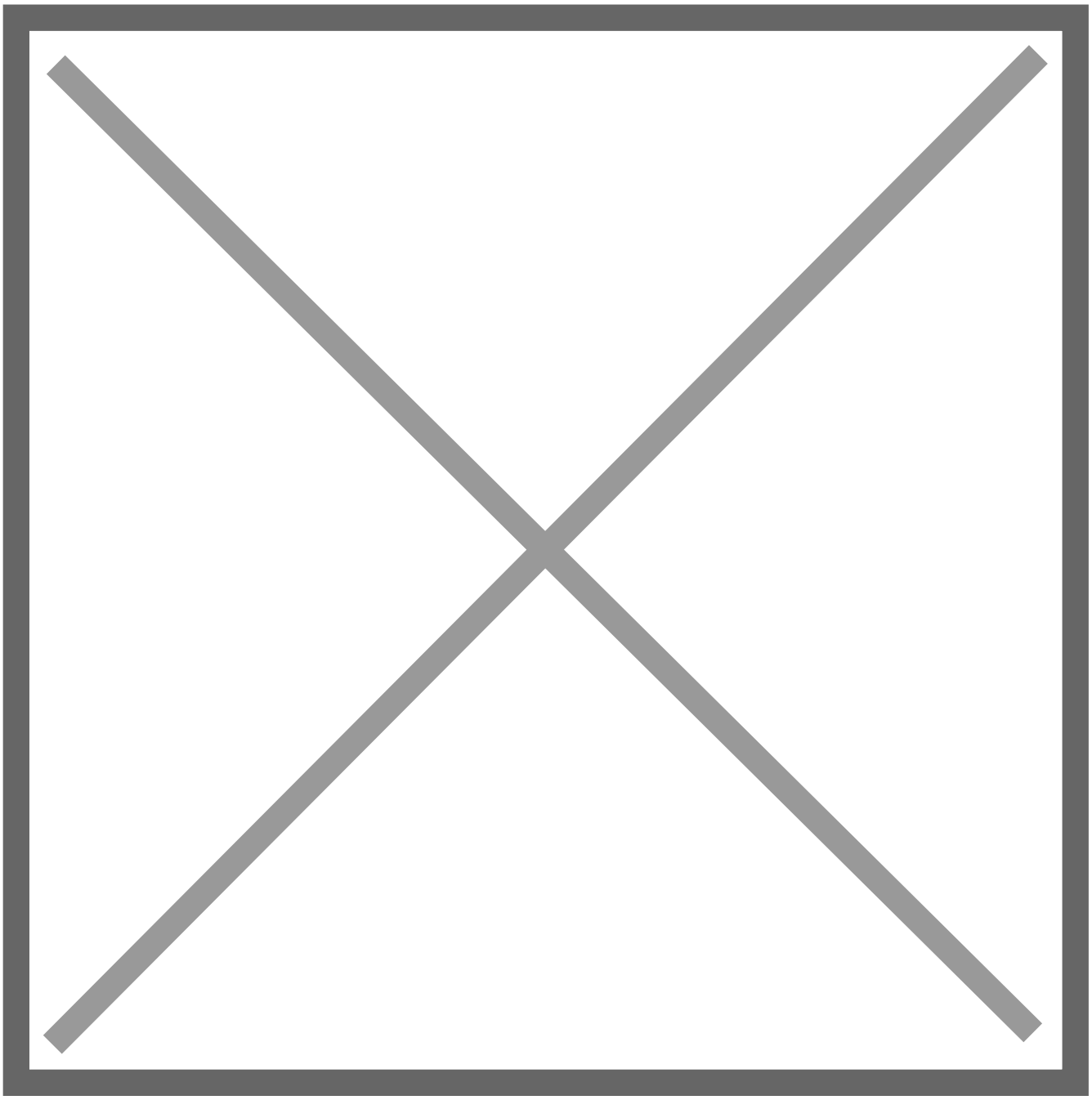
На тестовом рабочем месте, включенном в домен, запустите команду `gpresult` для проверки применения GPO (далее мы подробнее рассмотрим `gpresult`).

```
PS C:\Windows\system32> gpresult /H c:\gpreport.htm
```

Посмотрите html-файл и убедитесь, что настройки GPO применились (столбец Winning GPO):



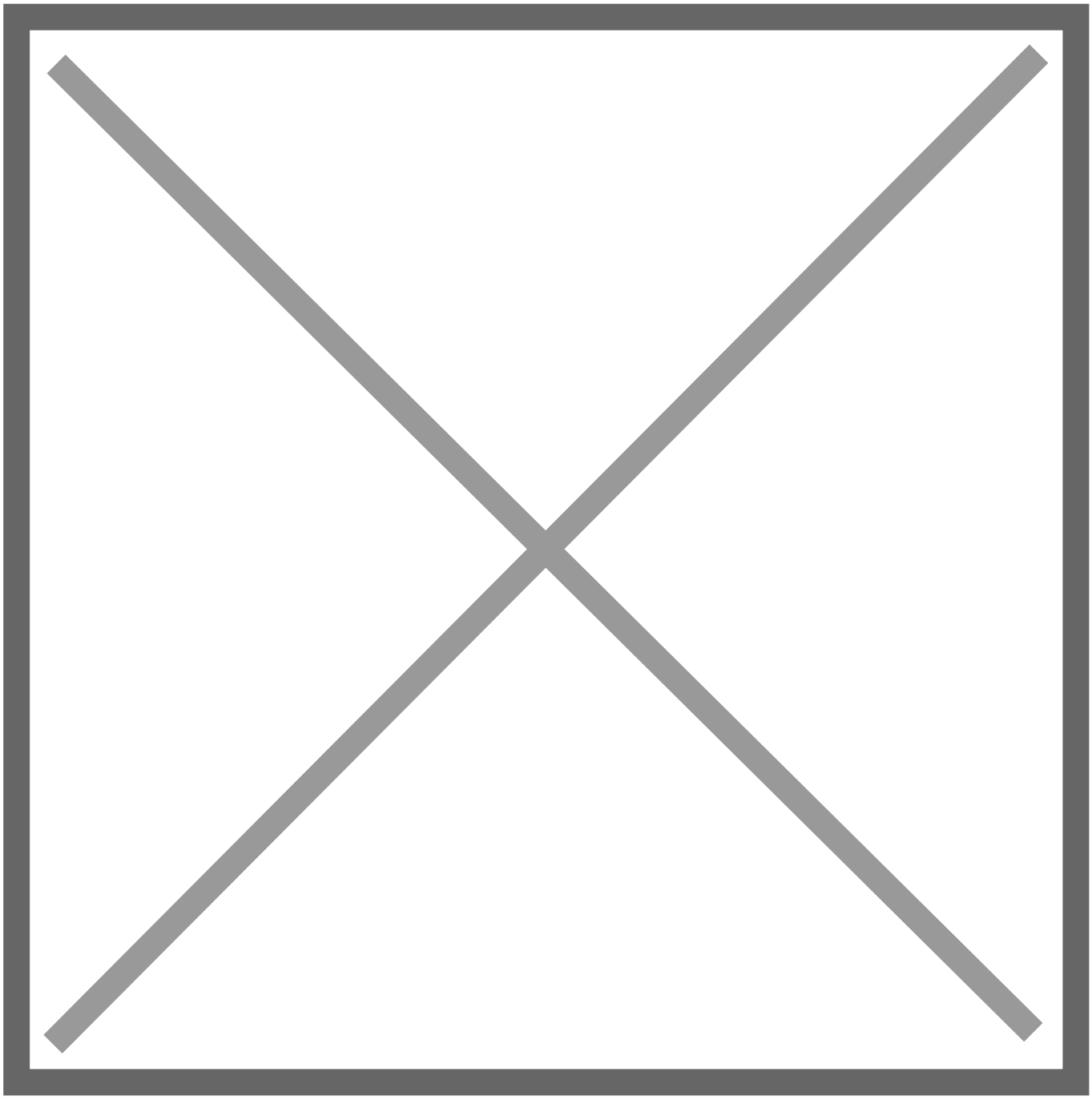
Вы также можете проверить локальный редактор групповых политик (gpedit.msc), чтобы вручную проверить настройки:



?????????? ???????? ????????? ????????

Как упоминалось ранее, объекты групповой политики могут использоваться для проведения атак. Эти атаки могут включать добавление дополнительных прав к учетной записи пользователя, добавление локального администратора на хост или создание немедленного запланированного задания для запуска вредоносной команды, такой как изменение членства в группе, добавление новой учетной записи администратора, установка обратной оболочки. соединение или даже установку целевого вредоносного ПО по всему домену. Эти атаки обычно происходят, когда у пользователя есть права, необходимые для изменения объекта групповой политики, который применяется к подразделению, содержащему либо учетную запись пользователя, которую мы контролируем, либо компьютер.

Ниже приведен пример пути атаки на GPO с помощью инструмента BloodHound. В данном примере группа Domain Users может изменять объект групповой политики Disconnect Idle RDP из-за членства в вложенной группе. Далее мы можем посмотреть, к каким подразделениям применяется этот объект групповой политики, и сможем ли мы использовать эти права для получения контроля над администратором или администратором домена или компьютером (сервером, контроллером домена или критически важным хостом) и двигаться дальше, чтобы повысить привилегии внутри домена:



???????? ???????????? GPO

После того как мы изучили основы GPO и их управления с помощью GPMC, перейдем к просмотру и проверке применения этих групповых политик на конкретные объекты и системы.

???????? ? RSoP: ??????????? ????????? ? ??????? ?? ????????? ??????

Результативная политика (Resultant Set Of Policy, RSoP):

- RSoP — это инструмент для понимания того, какие групповые политики были применены к компьютеру или пользователю, а также для диагностики проблем с политиками.
- RSoP может быть использован в графическом интерфейсе через MMC (Microsoft Management Console), запустив rsop.msc, или с помощью команды в PowerShell.

????????????? ??????? gpresult

`gpresult` — это командная утилита, которая показывает RSoP данных для локального или удаленного компьютера и пользователей. Основные параметры команды включают:

Parameter	Description
/s `<system>`	Для обозначения имени или IP-адреса удаленного хоста, используется без указания маски. Значение по умолчанию - локальный хост.
/u `<username>`	Для использования определенной УЗ для выполнения команды. Значение по умолчанию - текущий пользователь.
/p `[<password>]`	Для использования определенного пароля для УЗ, определенной в параметре **/u**. Если использовать **/u** без **/p**, **gpresult** запросит пароль. Параметр нельзя использовать с **/x** или **/h**.
/user `[<targetdomain>\]<targetuser>]`	Определяет пользователя, чьи RSoP данные нужно вывести.
/scope `{user | computer}`	Выводит данные RSoP либо для пользователя, либо для компьютера. Если /scope не используется, то **gpresult** выводит данные RSoP и для пользователя, и для компьютера вместе.
`[/x | /h] <filename>`	Для создания детального HTML или XML-отчета. Не может использоваться с **/u**, **/p**, **/r**, **/v**, or **/z**.

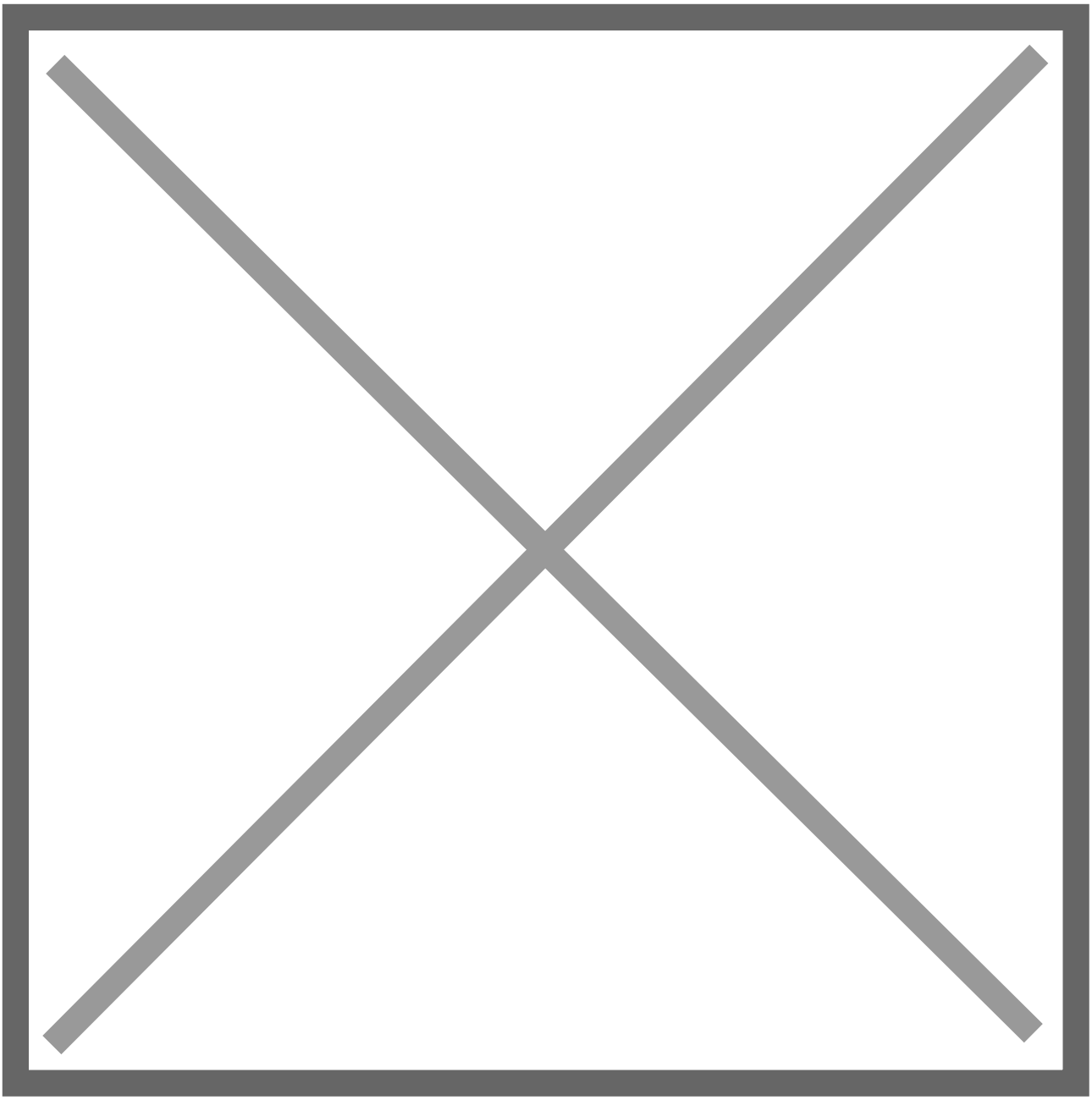
Parameter	Description
/f	Для перезаписи имени файла, которое используется при создании отчета с помощью **/x** или **/h**.
/r	Выводит суммированные данные RSoP.
/v	Отображает подробную информацию о политике.
/z	Отображает всю возможную информацию о групповой политике.
/?	Для вывода помощи.

?????? ????????????? gpresult

```
PS C:\Windows\system32> gpresult /H c:\GPReport.html
```

Команда `gpresult /H GPReport.html` используется для создания отчета о результатах применения групповых политик (Group Policy Results Report) в формате HTML. Она позволяет получить подробную информацию о том, какие групповые политики были применены к конкретному пользователю или компьютеру в сети.

После выполнения этой команды будет создан файл с именем "GPReport.html", который содержит подробный отчет о результатах применения групповых политик. В этом отчете вы найдете информацию о примененных политиках, их источниках, примененных параметрах и другие связанные с ними данные.



Этот отчет может быть полезен для отладки проблем с применением групповых политик, а также для проверки правильности конфигурации политик на конкретном компьютере или пользователе. Он позволяет администраторам подробно анализировать, какие политики были успешно применены, а какие не удалось применить, и выявлять возможные проблемы.

Отчет `GPReport.html` содержит следующую информацию:

1. **Общая информация**:
   - Имя пользователя и имя компьютера.
   - Дата и время создания отчета.
2. **Сводка результатов применения групповых политик**:
   - Общее количество примененных групповых политик.
   - Список успешно примененных политик.
   - Список неудачных попыток применения политик.

3. **Подробная информация о примененных групповых политиках**:
   - Имя и описание каждой примененной политики.
   - Источник (локальный GPO, сетевой GPO и т. д.).
   - Состояние применения (успешно, неудачно и т. д.).
   - Список параметров и их значений, примененных в рамках каждой политики.
4. **Информация о контексте применения политик**:
   - Пользователи и группы, к которым применялись политики.
   - Список компьютеров, к которым применялись политики.
5. **Дополнительная информация**:
   - Логи и ошибки, связанные с применением групповых политик.

GPUpdate ? ?????????????? ?????????? ???????

Команда `gpupdate` (Group Policy Update) используется для обновления групповых политик на компьютере или пользователе. Она запускает процесс обновления настроек групповых политик с сервера домена или локального хранилища групповых политик.

Вот основные задачи и цели команды `gpupdate`:

1. **Применение изменений групповых политик**: когда администратор вносит изменения в групповые политики в Active Directory, они не сразу применяются на клиентских компьютерах. Команда gpupdate позволяет немедленно обновить настройки групповых политик на компьютере или пользователе, чтобы применить изменения.
2. **Решение проблем с настройками**: иногда возникают ситуации, когда изменения в групповых политиках не применяются корректно на клиентских компьютерах. Запуск gpupdate может помочь в решении таких проблем путем принудительного обновления политик с помощью ключа `/force`.
3. **Отладка и тестирование**: во время разработки и тестирования групповых политик администраторы могут использовать gpupdate, чтобы немедленно применить изменения и убедиться, что они работают ожидаемым образом.
4. **Синхронизация настроек с доменом**: когда компьютер или пользователь подключаются к домену, они получают групповые политики с контроллера домена. gpupdate обновляет эти настройки, чтобы убедиться, что они соответствуют текущему состоянию в домене.
5. **Синхронизация настроек с локальным хранилищем**: Для компьютеров, работающих в автономном режиме или в отсутствие подключения к домену, gpupdate обновляет настройки с локального хранилища групповых политик.

???????? ??????? GPO ? ??????? ??????? Windows (eventvwr.msc)

Event Viewer Microsoft Management Console (MMC, eventvwr.msc) — консоль просмотра событий Windows. Это инструмент в операционной системе Windows, который позволяет администраторам просматривать, анализировать и управлять журналами событий компьютера.

Чтобы открыть **eventvwr.msc** и найти журналы, связанные с Group Policy, выполните следующие шаги:

1. **Откройте Консоль просмотра событий**:
   - Нажмите Win + R для открытия диалогового окна "Выполнить".
   - Введите eventvwr.msc.
   - Или щелкните правой кнопкой мыши на кнопке Пуск и выберите "Консоль просмотра событий".
2. **Найдите журналы, связанные с Group Policy**:
   - В левой панели Консоли просмотра событий откройте раздел "Журналы Windows".
   - Разверните раздел "Журналы Windows", чтобы увидеть список доступных журналов.
   - Журналы, связанные с Group Policy, обычно находятся в разделе "Приложение" или "Система".
3. **Анализируйте журналы событий Group Policy**:
   - Чтобы найти события, связанные с Group Policy, щелкните на соответствующем журнале (например, "Приложение").
   - Используйте фильтры или поиск, чтобы отфильтровать события, связанные с Group Policy. Обычно в журнале будут присутствовать события с источником "Group Policy" или "GroupPolicy".
4. **Проанализируйте события и сообщения**:
   - Просмотрите события, чтобы понять, какие политики были применены, успешно или с ошибками.
   - Изучите сообщения об ошибках или предупреждениях, чтобы выявить проблемы с применением Group Policy на компьютере или в сети.

??????? ??? ???????????? ? ??????? GPO

????????????? gpresult ??? ???????? ?????? ? ??????????? ????????? ? ??????????? ? HTML ????

Чтобы создать отчет о примененных групповых политиках (Group Policy Objects, GPO) для пользователя или компьютера и сохранить его в HTML-файл, используется инструмент командной строки `gpresult`. Для работы с gpresult необходимо иметь права администратора на локальной машине или в домене, а также работать на компьютере на базе Windows.

Вот как может выглядеть использование gpresult:

1. Откройте командную строку с правами администратора.

2. Введите следующую команду для создания отчета для текущего пользователя и его компьютера:

```
PS C:\Windows\system32> gpresult /H GPReport.html
```

Эта команда выполнит анализ примененных групповых политик и сохранит результат в файл `GPReport.html` в текущей директории.

3. Если хотите создать отчет только для компьютера или только для пользователя, используйте ключ `/SCOPE`, например:

- для компьютера:

```
PS C:\Windows\system32> gpresult /SCOPE COMPUTER /H GPReport_Computer.html
```

- для пользователя:

```
PS C:\Windows\system32> gpresult /SCOPE USER /H GPReport_User.html
```

4. По умолчанию отчет будет создан для текущего пользователя. Если необходимо создать отчет для другого пользователя, используйте ключ `/USER`, например:

```
PS C:\Windows\system32> gpresult /USER имя_пользователя /H GPReport_OtherUser.html
```

Замените "имя_пользователя" на фактическое имя пользователя, для которого нужно сгенерировать отчет.

Открыть созданный HTML-файл можно в любом веб-браузере, чтобы проанализировать результаты.

?????????????? ?????????? ??????? ????? gpupdate, ? ??? ??? ???????? ??? ?? ???????????? ??????????

Одним из ключевых навыков является использование команды `gpupdate`, которая позволяет принудительно инициировать процесс обновления групповых политик. Это бывает полезно в ситуациях, когда изменения в политиках не применяются как ожидалось, и вам нужно вручную запустить процесс обновления, чтобы убедиться, что последние изменения были корректно распространены на пользователей и компьютеры в сети.

Вот основы, которые можно рассмотреть:

1. Для выполнения команды `gpupdate` откройте командную строку. Можно использовать "Командную строку" или "Windows PowerShell".

2. Введите команду:

```
PS C:\Windows\system32> gpupdate
```

Это приведет к обновлению политик как для пользователя, так и для компьютера. По умолчанию gpupdate обновляет все политики, если какие-то политики были изменены, они будут применены с этой командой.

3. Если вы хотите обновить только пользовательские или только компьютерные политики, используйте следующие команды:

Для пользовательских политик:

```
PS C:\Windows\system32> gpupdate /target:user
```

Для компьютерных политик:

```
PS C:\Windows\system32> gpupdate /target:computer
```

4. Иногда может быть необходимо принудительно переприменить все связанные политики без учета их последнего времени обновления, для этого используйте ключ /force:

```
PS C:\Windows\system32> gpupdate gpupdate /force
```

5. После запуска `gpupdate` система может потребовать перезагрузку или выход пользователя из системы, если некоторые политики не могут быть обновлены на лету. В этом случае будет предоставлен запрос с выбором выполнения этого действия сразу или отложить его на более удобное время.

Использование `gpupdate` помогает решать проблемы с политиками, которые не применялись должным образом, путем их принудительного обновления, что позволяет администраторам быстро реагировать на изменения в конфигурации без ожидания следующего цикла автоматического обновления политик, и проверять результаты изменений в реальном времени.

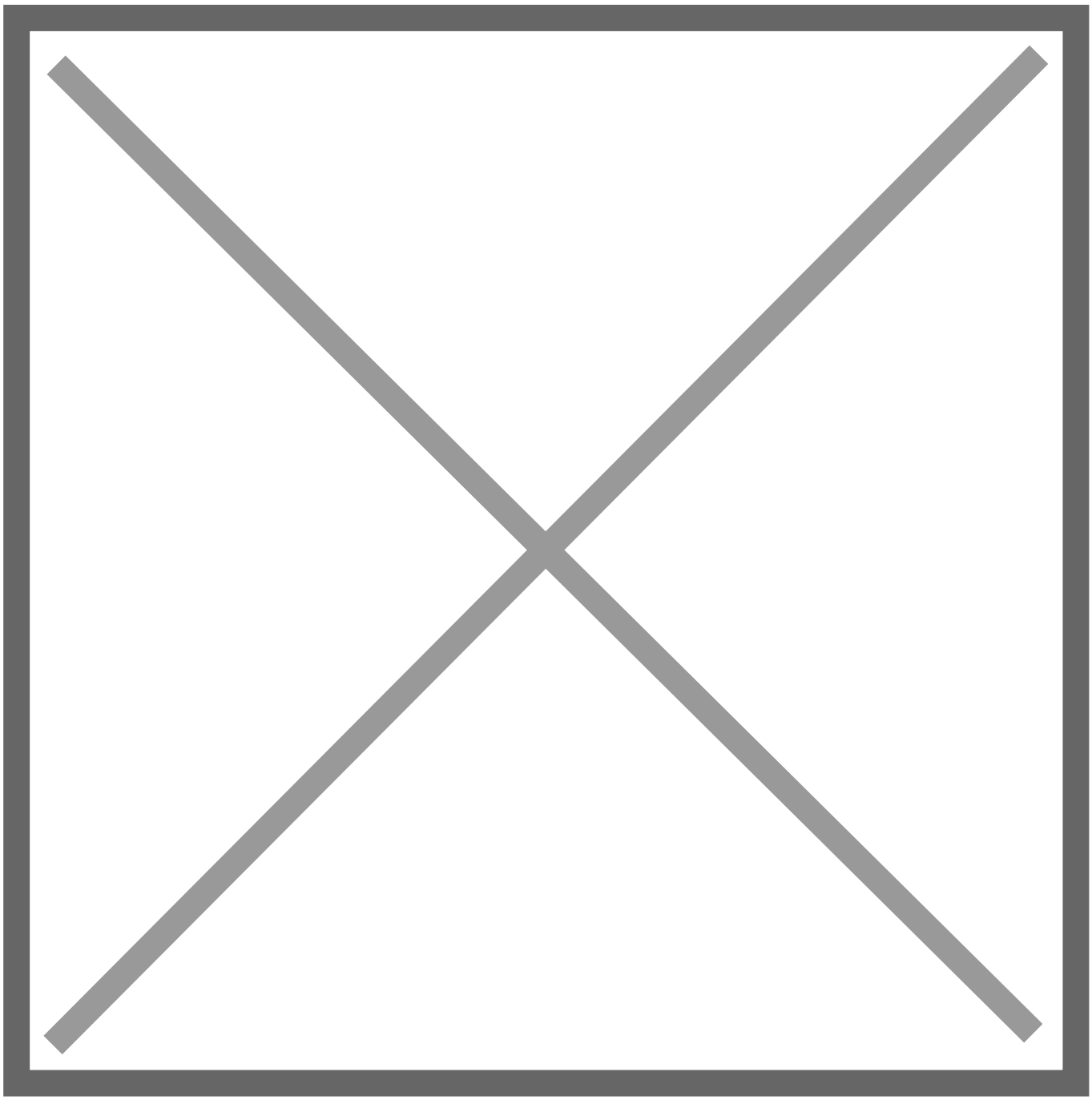
??????? ?????????? ????????? ????????

При создании нового объекта групповой политики параметры не применяются автоматически сразу. Windows выполняет периодические обновления групповой политики, которые по умолчанию выполняются каждые 90 минут со случайным смещением +/- 30 минут для пользователей и компьютеров. По умолчанию период обновления контроллеров домена составляет всего 5 минут. При создании и связывании нового объекта групповой политики может пройти до 2 часов (120 минут), прежде чем настройки вступят в силу. Это случайное смещение +/- 30 минут установлено, чтобы избежать перегрузки контроллеров домена, поскольку все клиенты одновременно запрашивают групповую политику у контроллера домена.

Можно изменить интервал обновления по умолчанию в самой групповой политике. Кроме того, мы можем ввести команду `gpupdate /force`, чтобы запустить процесс обновления. Эта команда сравнит объекты групповой политики, применяемые в настоящее время на компьютере, с контроллером домена и либо изменит, либо пропустит их в зависимости от того, изменились ли они с момента последнего автоматического обновления.

Мы можем изменить интервал обновления с помощью групповой политики, открыв **Computer Configuration -> Policies -> Administrative Templates -> System -> Group Policy** и выбрав **Set Group Policy refresh interval for computers**.

Стоит отметить, что хоть интервал и можно изменить, его не следует настраивать слишком часто, иначе это может вызвать перегрузку сети, что приведет к проблемам репликации.



?????? ? ??????????? ?????????

???????? ??????? ??????? ?? ??????? ?????? GPO

Важным навыком является проверка Журнала событий (Event Viewer) на предмет ошибок, связанных с GPO.
Журнал событий Windows содержит записи о всех важных событиях системы, включая ошибки, предупреждения и информационные сообщения от различных служб и компонентов

операционной системы, в том числе и связанные с групповыми политиками.

- В Журнале событий раскройте раздел "Журналы Windows", а затем перейдите в подраздел "Система". Здесь вы увидите все системные события. Чтобы сузить круг поиска, можно использовать фильтр - "Фильтр текущего журнала...".
- В фильтре можно задать параметры для поиска конкретных событий GPO. Введите источник события, такой как GroupPolicy, чтобы увидеть только события, связанные с групповыми политиками.
- Найдите и проанализируйте ошибки, связанные с GPO. Их идентификаторы (ID события) и источник (обычно это Microsoft-Windows-GroupPolicy) помогут вам узнать больше о каждом конкретном случае.

К примеру у нас есть некий список, что нужно для устранения:

1. **Проверьте подробности события**: Используйте Журнал событий для поиска ошибок, связанных с Group Policy. Обратите внимание на ID события, уровень серьезности, сообщение об ошибке и любые предлагаемые действия или коды.
2. **Проверка связи с доменным контроллером**: Убедитесь, что компьютер может связываться с доменным контроллером. Используйте ping, nslookup, и другие сетевые утилиты для диагностики проблем с сетью.
3. **Фильтрация GPO**: Проверьте, нет ли настроек фильтрации на ваши групповые политики, которые могут исключать определенные объекты из области их действия. Убедитесь, что WMI-фильтры и целевая выборка работают корректно и не ограничивают применение GPO.
4. **Проверка разрешений GPO**: Проверьте, имеют ли учетные записи пользователей или компьютеров соответствующие разрешения для применения групповой политики. Необходимыми разрешениями обычно являются "Прочитать" и "Применить групповую политику".
5. **Конфликтующие и перезаписывающие настройки**: Рассмотрите возможность того, что одна политика перезаписывает другую. Используйте инструменты моделирования и планирования Group Policy Management Console (GPMC) для анализа результата применения политик.
6. **Восстановление синхронизации**: Иногда GPO могут не применяться из-за проблем с репликацией или синхронизацией. Убедитесь, что все доменные контроллеры синхронизированы и актуальны.
7. **Просмотр журналов на стороне сервера**: Полезно проверить журналы на доменном контроллере, чтобы увидеть, возникали ли там ошибки, которые могли повлиять на распространение политик.
8. **Обновление шаблонов административных шаблонов (ADM/ADMX)**: Устаревшие или поврежденные файлы шаблонов могут вызвать проблемы с применением политик. Проверьте, что используются актуальные версии ADM/ADMX-файлов.
9. **Проверка наличия последних обновлений**: Убедитесь, что на клиентских компьютерах и доменных контроллерах установлены последние обновления операционной системы, поскольку в них могут содержаться патчи для известных проблем с GPO.

????? ???????????? ??? ??????????? ???????????? ??????????? ???????????? ? ??????? ?????????

Microsoft Security Compliance Toolkit (MSCT) — это набор инструментов и руководств, предоставляемых Microsoft для помощи организациям в обеспечении безопасности и соответствия в их информационных системах, особенно в операционных системах Windows.

В рамках Microsoft Security Compliance Toolkit доступны следующие ресурсы:

1. **Готовые конфигурации безопасности**: MSCT включает в себя готовые наборы рекомендаций по настройке безопасности для различных продуктов Microsoft, таких как операционные системы Windows, серверы и приложения. Эти наборы конфигураций, называемые бенчмарками безопасности (Security Baselines), содержат набор рекомендуемых настроек безопасности, которые можно применить с помощью групповых политик (GPO) для обеспечения соответствия и улучшения безопасности в организации.
2. **Инструменты анализа и реализации**: В состав Toolkit входят инструменты для анализа безопасности существующих систем и для реализации рекомендуемых настроек безопасности. Например, инструменты Security Compliance Toolkit могут автоматически проверить соответствие существующих систем установленным бенчмаркам безопасности и предоставить рекомендации по улучшению безопасности.
3. **Документация и руководства**: MSCT включает в себя подробные руководства по применению бенчмарков безопасности и использованию инструментов Toolkit. Эти руководства помогают администраторам понять рекомендации по настройке безопасности и успешно применить их в своей среде.

Бенчмарки безопасности, предоставляемые в составе Toolkit, часто используются для настройки безопасности с помощью групповых политик. Администраторы могут импортировать бенчмарки безопасности в GPO и применить их настройки к компьютерам и пользователям в своей сети, чтобы обеспечить соответствие установленным стандартам безопасности и улучшить защиту систем от угроз.

Более подробную информацию можно посмотреть по ссылке.

???????? ???????

```
Copy-GPO -SourceName "GPO to copy" -TargetName "Name"
```

Копирует групповую политику "GPO to copy" для использования в качестве новой политики с именем "Name".

```
New-GPLink -Name "Security Analysts Control" -Target "ou=Security Analysts,ou=IT,OU=HQ-
NYC,OU=Employees,OU=Corp,dc=SECOPS,dc=LOCAL" -LinkEnabled Yes
```

Создает новую групповую политику и связывает ее с выбранным подразделением или группой безопасности.

```
Set-GPLink -Name "Security Analysts Control" -Target "ou=Security Analysts,ou=IT,OU=HQ-
NYC,OU=Employees,OU=Corp,dc=SECOPS,dc=LOCAL" -LinkEnabled Yes
```

Связывает существующую групповую политику с соответствующим подразделением или группой безопасности.

Revision #2
Created 17 October 2025 13:00:59 by Admin
Updated 27 October 2025 14:39:28 by Admin