

Администрирование Windows Server 2012

Лабораторная работа № 7. Аудит и проверка подлинности

Аудит – это важный компонент системы безопасности. В процессе аудита информация об указанной активности на предприятии заносится в журнал Безопасность Windows (Windows Security), который впоследствии можно анализировать. Аудит может вести запись успешной деятельности, документируя все изменения, а также фиксировать неудачные и потенциально вредоносные попытки получить доступ к ресурсам предприятия. В процессе аудита используются три средства управления: политика аудита, параметры аудита в объектах и журнал Безопасность (Security).

Для настройки аудита необходимо определить параметр политики. Дважды щелкните любой параметр политики и установите флажок Определить следующие параметры политики (Define These Policy Settings). Затем укажите ведение аудита успеха, отказа или обоих типов событий.

Контроллеры домена выполняют аудит большинства успешно выполненных важных событий Active Directory. Поэтому ведется запись всех событий создания пользователя, изменения пароля пользователя, входа в домен и извлечения сценариев входа пользователя.

Но поскольку по умолчанию проверяются не все события отказа, может потребоваться провести дополнительный аудит отказов на основе политик безопасности и требований организации. Например, аудит неудачных попыток входа выявляет попытки несанкционированного доступа к домену путем многократного входа с помощью учетной записи пользователя домена без данных о пароле. События управления отказами доступа учетных записей могут помочь определить попытки манипулирования членством в группе с уязвимой безопасностью.

Часть 1: Конфигурирование параметров аудита

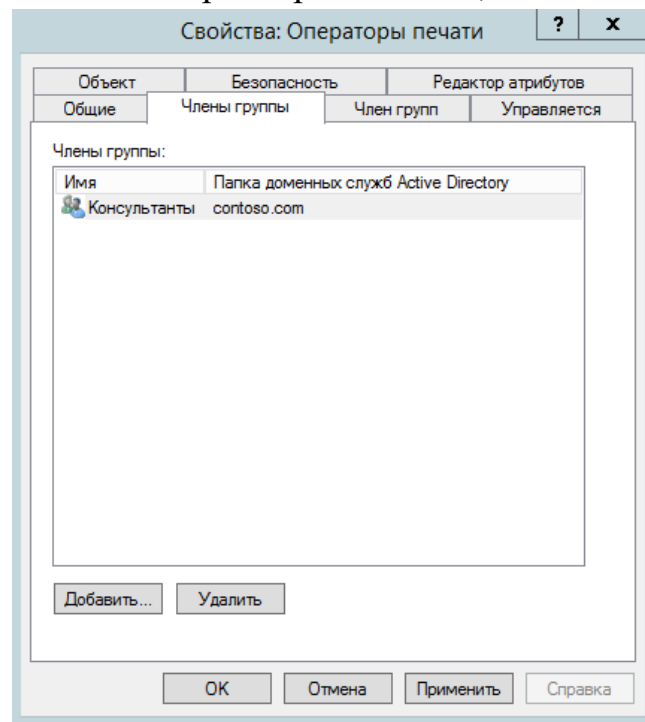
Для выполнения аудита доступа к файлу или папке, добавив записи аудита в список SACL файла или папки. Чтобы получить доступ к списку SACL и его записям аудита, откройте диалоговое окно Свойства (Properties), перейдите на вкладку Безопасность (Security), щелкните кнопку Дополнительно (Advanced) и перейдите на вкладку Аудит (Auditing). Откроется диалоговое окно Дополнительные параметры безопасности (Advanced Security Settings).

Для того чтобы добавить запись, щелкните кнопку Изменить (Edit). Откроется вкладка Аудит (Auditing) в режиме редактирования. Щелкните кнопку Добавить (Add) и выберите пользователя, группу или компьютер для аудита. Затем в диалоговом окне Элемент аудита (Auditing Entry) укажите тип аудита доступа к объекту.

В предложенных далее упражнениях предлагается отконфигурировать параметры аудита, включить политики аудита доступа к объектам и отфильтровать конкретные события в журнале Безопасность (Security). Бизнес-цель состоит в мониторинге папки с конфиденциальными данными, к которой не должны получать доступ пользователи из группы Консультанты. Кроме того, необходимо отконфигурировать аудит для отслеживания изменений членства группы Администраторы домена (Domain Admins).

Прежде всего нужно выполнить в среде следующие подготовительные шаги:

- на диске С создать папку Конфиденциальные данные;
- создать глобальную группу безопасности Консультанты;
- добавить группу Консультанты в группу Операторы печати (Print Operators) — благодаря этому пользователь в группе Консультанты сможет локально входить на машину SERVER01, которая в данном упражнении является контроллером домена;



- создать пользователя Джеймс Фаин и добавить его в группу Консультанты.

Упражнение 1. Настройка разрешений и параметров аудита

Необходимо отконфигурировать разрешения папки Конфиденциальные данные для запрета доступа пользователям из группы Консультанты, затем включить для них аудит попыток получить доступ к этой папке.

1. Войдите на машину SERVER01 как администратор.
2. Откройте окно свойств папки C:\Конфиденциальные данные и перейдите на вкладку Безопасность (Security).
3. Щелкните кнопку Изменить (Edit), а затем Добавить (Add).
5. Введите имя группы Консультанты и щелкните ОК.

6. Установите флажок Запретить напротив разрешения Полный доступ.
7. Последовательно щелкните кнопки Применить (Apply) и Да (Yes), чтобы подтвердить запрет разрешения.
8. Для того чтобы закрыть диалоговое окно Разрешения, щелкните ОК.
9. Щелкните Дополнительно .
10. Перейдите на вкладку Аудит.
11. Щелкните Изменить, а затем Добавить.
13. Введите имя Консультанты и щелкните ОК.
14. Установите флажок Отказ напротив Тип и выберите разрешение Полный доступ.
15. Закройте все диалоговые окна.

Упражнение 2. Включение политики аудита

Поскольку машина SERVER01 является контроллером домена, для включения аудита используется ранее созданный объект групповой политики Политика безопасности DC. На автономном сервере применяется оснастка Локальная политика безопасности (Local Security Policy) или объект GPO, под область действия которого подпадает сервер.

1. Откройте консоль Управление групповой политикой (Group Policy Management) и выберите контейнер Объекты групповой политики (Group Policy Objects).
2. Щелкните правой кнопкой мыши объект **Default Domain Controllers Policy** и выполните команду Изменить (Edit).
3. Разверните узел Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Локальные политики\Политика аудита (Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy).
4. Дважды щелкните параметр политики Аудит доступа к объектам.
5. Установите флажок Определить следующие параметры политики (Define These Policy Settings).
6. Установите флажок Отказ (Failure).
7. Щелкните ОК, а затем закройте консоль.
8. Для обновления политики и применения всех параметров откройте окно командной строки и введите команду *gpupdate*.

Упражнение 3. Генерирование событий аудита

Теперь следует попытаться получить доступ к папке Конфиденциальные данные как член группы Консультанты.

1. Войдите на машину SERVER01 как пользователь Джеймс Файн.
2. Откройте окно Мой компьютер (My Computer) и попытайтесь открыть папку C:\Конфиденциальные данные.

3. Создайте текстовый файл на рабочем столе и попытайтесь вырезать и вставить его в папку Конфиденциальные данные.

Упражнение 4. Анализ журнала безопасности

Теперь нужно просмотреть информацию о попытках консультантов получить доступ к папке Конфиденциальные данные.

1. Войдите на машину SERVER01 как администратор.

2. В группе Администрирование откройте оснастку Просмотр событий.

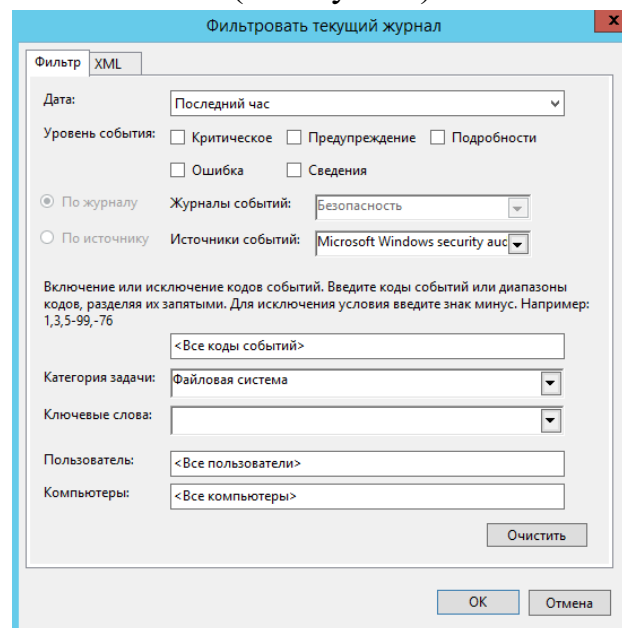
3. Разверните узел Журналы Windows\Безопасность (Windows Logs\Security). Какие типы событий отображаются в журнале Безопасность (Security)?

Помните, что политики позволяют выполнять аудит многочисленных действий, связанных с безопасностью, включая аудит доступа к службе каталогов, управление учетными записями, входа и т. д. Источником событий в столбце Источник (Source) является аудит безопасности Microsoft Windows.

4. Для фильтрации журнала и ограничения области поиска на панели Действия (Actions) щелкните ссылку Фильтр текущего журнала.

5. Отконфигурируйте фильтр для ограничения поиска.

Чтобы указать событие для локализации, используйте следующие параметры: события за последний час с источником событий Microsoft Windows security auditing и категорией задачи Файловая система (File System).



6. Отконфигурируйте фильтр журнала безопасности для извлечения последних событий файловой системы.

7. Щелкните ОК.

8. На панели Действия (Actions) щелкните ссылку Сохранить файл отфильтрованного журнала (Save Filter Log As).

9. На панели Избранные ссылки (Favorite Links) диалогового окна Сохранить файл (Save As) щелкните ссылку Рабочий стол (Desktop).

10. Щелкните раскрывающийся список Тип файла (Save As Type) и выберите тип Текст (Text).

11. В текстовое поле Имя файла (File Name) введите имя Экспорт журнала аудита.

12. Щелкните кнопку Сохранить (Save).

13. В программе Блокнот (Notepad) откройте полученный текстовый файл и выполните поиск по ключевым словам C:\Конфиденциальные данные.

Маска доступа: 0x100081
Привилегии, используемые для проверки доступа: -
Число ограниченных ИД безопасности: 0"

Сведения	29.07.2026 18:28:36	Microsoft-Windows-Security-Auditing	4656	Файловая система	"Запрошен дескриптор объекта."
----------	---------------------	-------------------------------------	------	------------------	--------------------------------

Субъект:

ИД безопасности:	CONTOSO\dfine
Имя учетной записи:	dfine
Домен учетной записи:	CONTOSO
ИД входа:	0x1E84D

Объект:

Сервер объекта:	Security
Тип объекта:	File
Имя объекта:	C:\Конфиденциальные данные
Код дескриптора:	0x0

Упражнение 5. Аудит изменений службы каталогов

В этом упражнении используется аудит доступа к службе каталогов, которая по умолчанию включена в Windows Server 2012. Затем необходимо реализовать новый аудит изменений службы каталогов Windows Server 2012, чтобы отслеживать изменения группы администраторов домена.

1. Откройте оснастку Active Directory — пользователи и компьютеры.

2. Щелкните меню Вид и установите флажок Дополнительные параметры.

3. Выберите контейнер Users.

4. Щелкните правой кнопкой мыши группу Администраторы домена (Domain Admins) и выполните команду Свойства.

5. Перейдите на вкладку Безопасность и щелкните кнопку Дополнительно (Advanced).

6. Перейдите на вкладку Аудит и щелкните кнопку Добавить.

7. Введите имя группы Все.

8. Установите флажок Успех напротив разрешения Запись: Члены группы. Щелкните ОК.

9. Закройте диалоговое окно Дополнительные параметры безопасности, щелкнув ОК.

Вы назначили аудит всех изменений атрибута member группы Администраторы домена. Теперь внесите два изменения в членство группы.

10. Перейдите на вкладку Члены группы.

11. Добавьте пользователя Джеймса Файна и щелкните Применить (Apply).

12. Выберите пользователя Джеймса Файна, щелкните Удалить (Remove), а затем Применить (Apply).

13. Щелкните ОК, чтобы закрыть диалоговое окно Свойства: Администраторы домена.

14. Откройте журнал Безопасность (Security) и локализируйте события, сгенерированные при добавлении и удалении пользователя Джеймса Файна. Код события 4662. Просмотрите информацию на вкладке Общие.

В журнале указано, что пользователь (администратор) получил доступ К объекту Администраторы домена (Domain Admins) и применил операцию доступа Записать свойство. Само свойство отображено как глобальный уникальный идентификатор (GUID), с помощью которого нельзя сразу определить изменение атрибута member. Это событие также не содержит данных об изменении, внесенном в свойство.

Теперь следует включить новый аудит изменений службы каталогов Windows Server 2012.

15. Откройте окно командной строки и введите следующую команду:
auditpol /set /subcategory:"изменения службы каталогов" /success:enable

16. Откройте окно свойств группы Администраторы домена (Domain Admins) и добавьте в группу пользователя Джеймса Файна.

17. Вернитесь к оснастке Просмотр событий (Event Viewer) и обновите журнал Безопасность (Security). Должны отобразиться события Доступ к службе каталогов (Directory Service Access) с кодом 4662 и Изменения службы каталогов (Directory Service Changes) с кодом 5136. Если событие изменения службы каталогов не отображается, подождите несколько секунд и вновь обновите представление журнала.

18. Проанализируйте информацию в событии Изменения службы каталогов (Directory Service Changes).

Информация на вкладке Общие (General) четко указывает, что пользователь (администратор) внес изменение в объект Администраторы домена (Domain Admins) каталога, а именно: добавил пользователя Джеймса Файна.

Часть 2: Проверка подлинности и политика паролей

Когда пользователь входит в домен Active Directory, он вводит свое имя и пароль, а клиент применяет эти учетные данные для проверки подлинности пользователя, то есть подтверждения идентификации объекта пользователя в соответствии с его учетной записью в Active Directory.

В домене Windows Server 2012 пользователям необходимо изменять свои пароли каждые 42 дня, а пароль должен содержать как минимум семь символов и соответствовать требованиям сложности, включая использование трех из четырех элементов написания: верхнего регистра, нижнего регистра, цифр и особых

символов. Эти политики максимального срока действия, длины и сложности паролей — первые, с которыми администраторы и пользователи сталкиваются в домене Active Directory. Параметры по умолчанию редко настраиваются точно по требованиям безопасности в организации.

Политика паролей домена конфигурируется объектом GPO, в область действия которого попадает домен. В узле Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика паролей (Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies>Password Policy) этого объекта GPO можно отконфигурировать параметры политики, определяющие требования к паролям.

Пользователь должен изменить свой пароль в течение количества дней, указанного параметром политики Максимальный срок действия пароля. Когда пользователь вводит новый пароль, его длина сравнивается с количеством знаков в политике Минимальная длина пароля. Если включена политика Пароль должен соответствовать требованиям сложности (Password Must Meet Complexity Requirements), новый пароль должен содержать символы хотя бы трех из четырех типов:

- латинские заглавные буквы (от A до Z);
- латинские строчные буквы (от a до z);
- цифры (от 0 до 9);
- отличные от букв и цифр знаки (например, !, \$, #, %).

Если новый пароль соответствует требованиям, он пропускается через математический алгоритм, преобразующий пароль в так называемый *хэш-код*. Этот код уникален, следовательно два пароля не могут быть преобразованы в один хэш-код. Алгоритм, используемый для создания хэш-кода, называется односторонней функцией. Пароль нельзя извлечь из хэш-кода с помощью функции обратного преобразования. Поскольку в Active Directory хранится хэш-код, а не сам пароль, уровень безопасности учетной записи повышается.

Кроме того, в Active Directory может проверяться кэш предыдущих хэш-кодов пользователей, чтобы в качестве нового пароля пользователь не мог ввести старый. Количество старых паролей, с которыми сопоставляется новый пароль, определяется политикой Вести журнал паролей (Enforce Password History). По умолчанию в Windows поддерживаются 24 предыдущих хэш-кода.

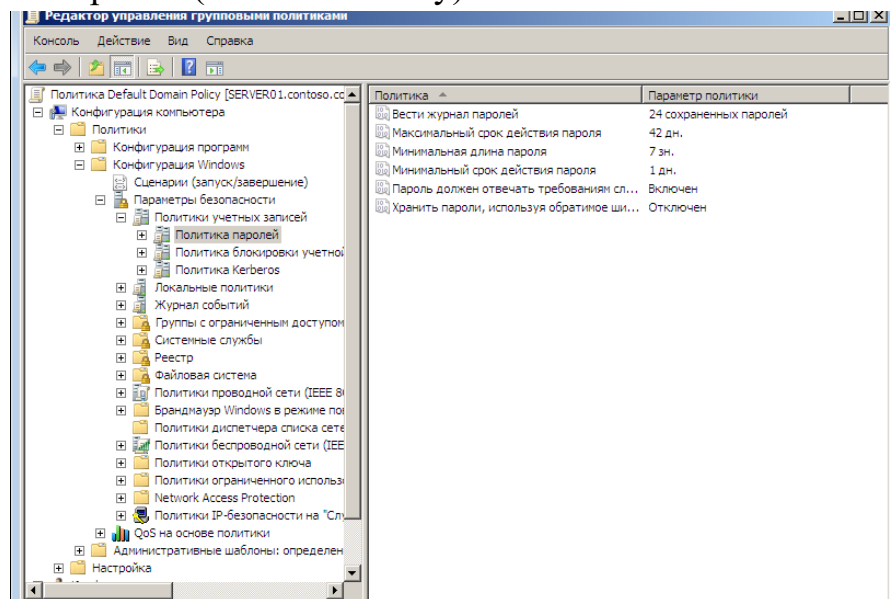
Упражнение 6. Настройка политики паролей и блокировки учетных записей в домене

В Active Directory для домена поддерживается один набор политик паролей и блокировки. Эти политики отконфигурированы в объекте GPO, в область действия которого попадает домен. Новый домен содержит объект GPO с именем Default Domain Policy, который связан с доменом и включает параметры политики по

умолчанию. Эти параметры можно изменить, отредактировав объект Default Domain Policy.

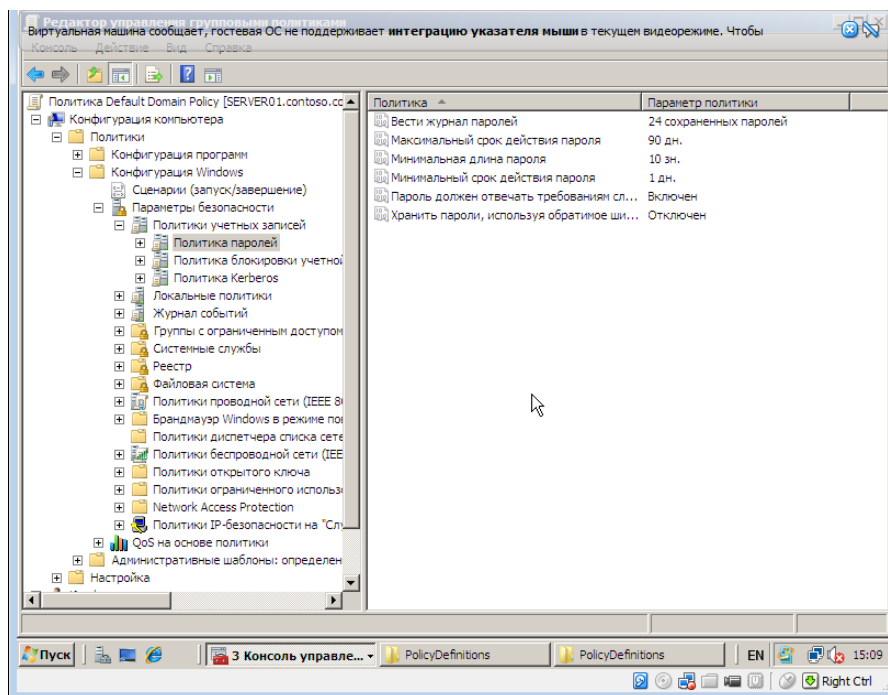
В этом упражнении вы модифицируете объект групповой политики Default Domain Policy для реализации политики паролей и блокировки пользователей в домене contoso.com.

1. Войдите на машину SERVER01 как Администратор.
2. В группе Администрирование (Administrative Tools) откройте консоль Управление групповой политикой.
3. Разверните узлы Лес (Forest), Домены (Domains), а затем узел домена contoso.com.
4. Под узлом contoso.com щелкните правой кнопкой мыши объект Default Domain Policy и примените команду Изменить (Edit). При этом может появиться уведомление об изменении параметров GPO.
5. Щелкните ОК. Откроется Редактор управления групповыми политиками.
6. Разверните узел Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Политики учетных записей (Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies) и выберите параметр Политика паролей (Password Policy).



7. В панели сведений консоли дважды щелкните следующие параметры безопасности и укажите такие значения:

- Максимальный срок действия пароля (Maximum Password Age): 90 дней;
- Минимальная длина пароля (Minimum Password Length): 10 знаков.

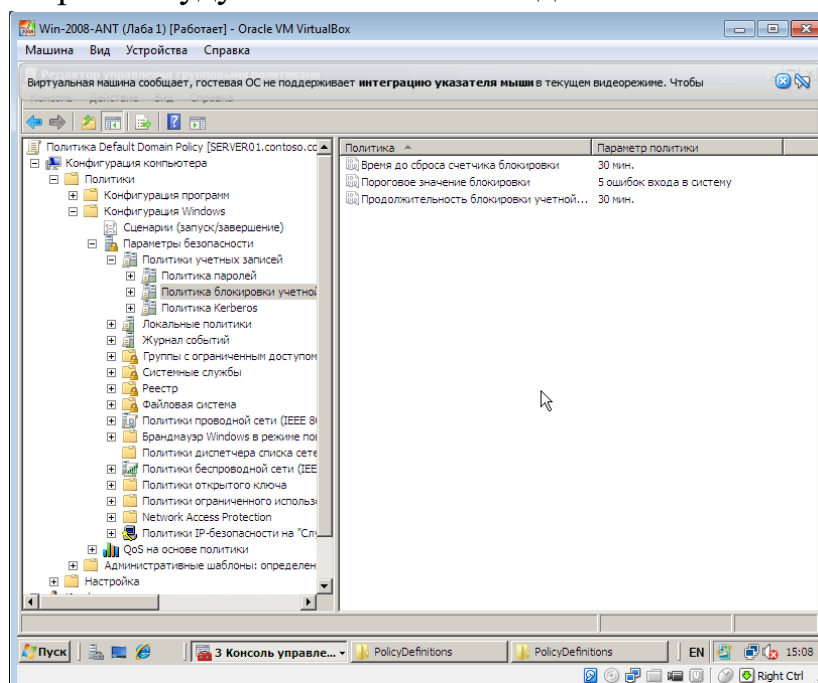


8. В дереве консоли выберите узел Политика блокировки учетной записи (Account Lockout Policy).

9. Дважды щелкните параметр политики Пороговое значение блокировки и задайте 5 ошибок входа в систему.

10. Откроется окно Предлагаемые изменения значений. Щелкните ОК.

Для параметров Продолжительность блокировки учетной записи и Время до сброса счетчика блокировки будут автоматически заданы значения 30 мин.



11. Закройте консоль Редактор управления групповыми политиками (Group Policy Management Editor).

12. Обновите параметры политик:

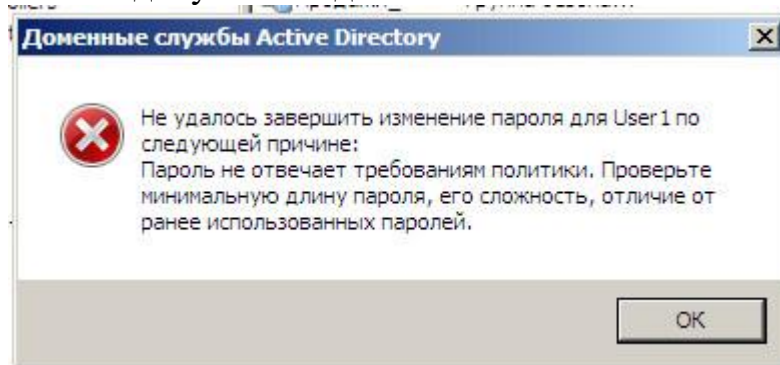
`cmd groupdate`

13. Зайдите в

Доменные службы AD DS пользователи и компьютеры

Найдите пользователя User1 и попытайтесь задать пароль:

- 1) Меньше минимально допустимой длины
- 2) Больше минимально допустимой длины



Упражнение 7. Настройка аудита событий входа учетной записи

В этом упражнении вы модифицируете объект групповой политики Default Domain Controllers Policy для аудита успешного и неудачного входа пользователей в домене.

1. Откройте консоль Управление групповой политикой.
2. Разверните узел Лес\Домены\contoso.com\Domain Controllers (Forest\Domains\contoso.com\Domain Controllers).
3. Щелкните правой кнопкой мыши объект Default Domain Controllers Policy и примените команду Изменить (Edit).

Откроется Редактор управления групповыми политиками.

4. Разверните узел Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Локальные политики и выберите папку Политика аудита.
5. Дважды щелкните параметр политики Аудит входа в систему.
6. Установите флажок Определить следующие параметры политики.
7. Установите флажки Успех (Success) и Отказ (Failure). Щелкните ОК.
8. Дважды щелкните параметр политики Аудит событий входа в систему.
9. Установите флажок Определить следующие параметры политики.
10. Установите флажки Успех (Success) и Отказ (Failure). Щелкните ОК.
11. Закройте Редактор управления групповыми политиками.
12. В главном меню (Start) щелкните значок Командная строка
13. Введите команду *gpupdate.exe /force*. Эта команда дает указание машине SERVER01 обновить свои политики, при этом будут применены новые политики аудита.

Упражнение 8. Генерирование событий входа учетной записи

В этом упражнении вы сгенерируете события входа учетной записи, используя при входе правильный и неправильные пароли.

1. Выйдите из системы SERVER01.

2. Попробуйте войти в систему, указав некорректный пароль для учетной записи Администратор (Administrator). Повторите попытку один или два раза.
3. Войдите на машину SERVER01 с использованием правильного пароля.

Упражнение 9. Анализ событий входа учетной записи

Выполняя данное упражнение, вы просмотрите события, которые были сгенерированы в упражнении 8.

1. В группе Администрирование (Administrative Tools) откройте оснастку Просмотр событий.
2. Разверните узел Журналы Windows (Windows Logs) и выберите журнал Безопасность.
3. Отыщите успешные и неудачные события.

Событие	Идентификатор	Значок в журнале
Успешный вход	4624	Обычно значок ключа
Неудачный вход	4625	Обычно значок замка

