

Практическое задание по работе с объектами AD и созданием политик GPO

Выполнил: Александр Ганицев

Задание

Вам необходимо произвести настройку Active Directory по следующему ТЗ:

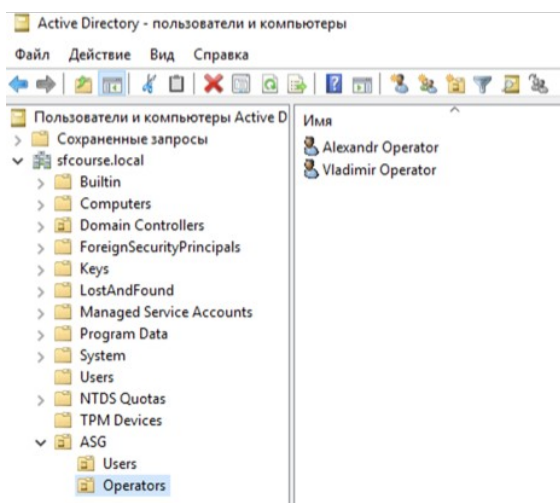
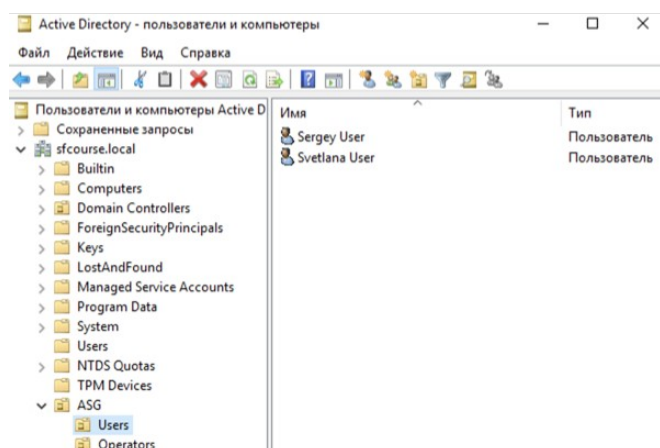
1. Создайте 4 пользователя с двумя функциональными ролями: «пользователь» и «оператор». Функциональные роли выражены в групповых объектах Active Directory (итого — 4 пользователя, по 2 в каждой группе).
2. Для каждой группы создайте групповую политику.
3. Для всех ролей в групповую политику включите следующие правила:
 - Минимальное количество символов в пароле — 8;
 - Необходимость спецсимволов в пароле — да;
 - Максимальное время жизни пароля — 45 дней.
4. Для роли «пользователь»:
 - Через групповую политику поставьте задний фон рабочего стола на ваш выбор.
 - Отключите возможность смены пароля.
 - Запретите редактирование реестра Windows.
5. Для роли «оператор»:
 - Через групповую политику поставьте задний фон рабочего стола на ваш выбор. Фон должен отличаться от изображения на рабочем столе «пользователя».
 - При входе «оператора» должен открываться PowerShell.
6. Включите KDC Armoring и поставьте значение TheMachineAccountQuota на «5».

УСЛОВИЯ РЕАЛИЗАЦИИ

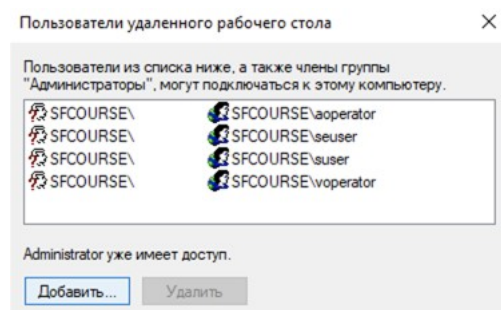
В качестве результата предоставьте (загрузите на GitHub и пришлите ссылку на репозиторий):

скриншоты наличия объектов в Active Directory;
скриншоты входа на SF_CLIENT под доменными пользователями с разными ролями;
созданные политики в текстовом виде (как вариант: вывод команд `gpresult /scope computer` и `gpresult /scope user` для каждой роли);
скриншот пользователя с SF_CLIENT (скрин рабочего стола);
скриншот оператора с SF_CLIENT (скрин рабочего стола);
скриншот предупреждения после попытки «пользователя» запустить regedit.

1. Созданы локальный филиал организации (подразделение) SFCOURSE – ASG с двумя подгруппами: “Пользователь” и “Оператор”.

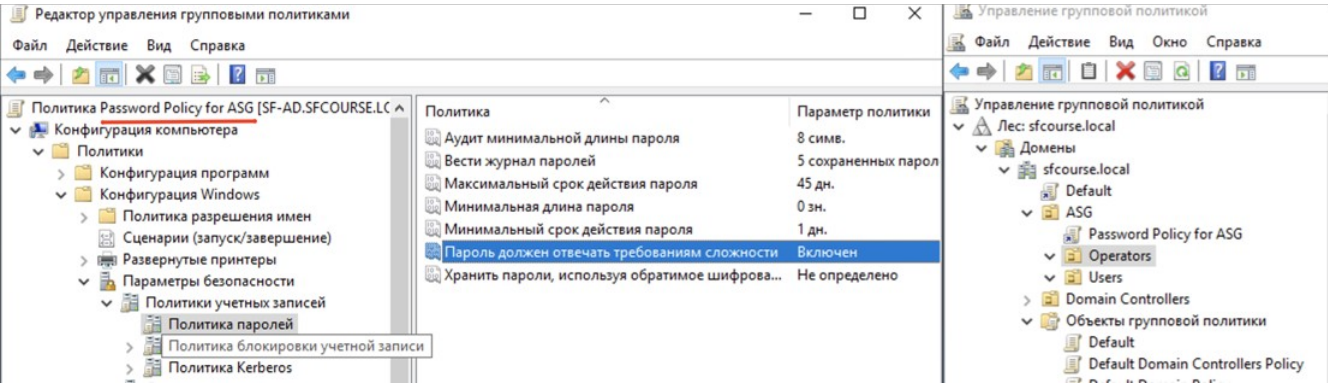


Добавлен удалённый доступ для созданных учётных записей.

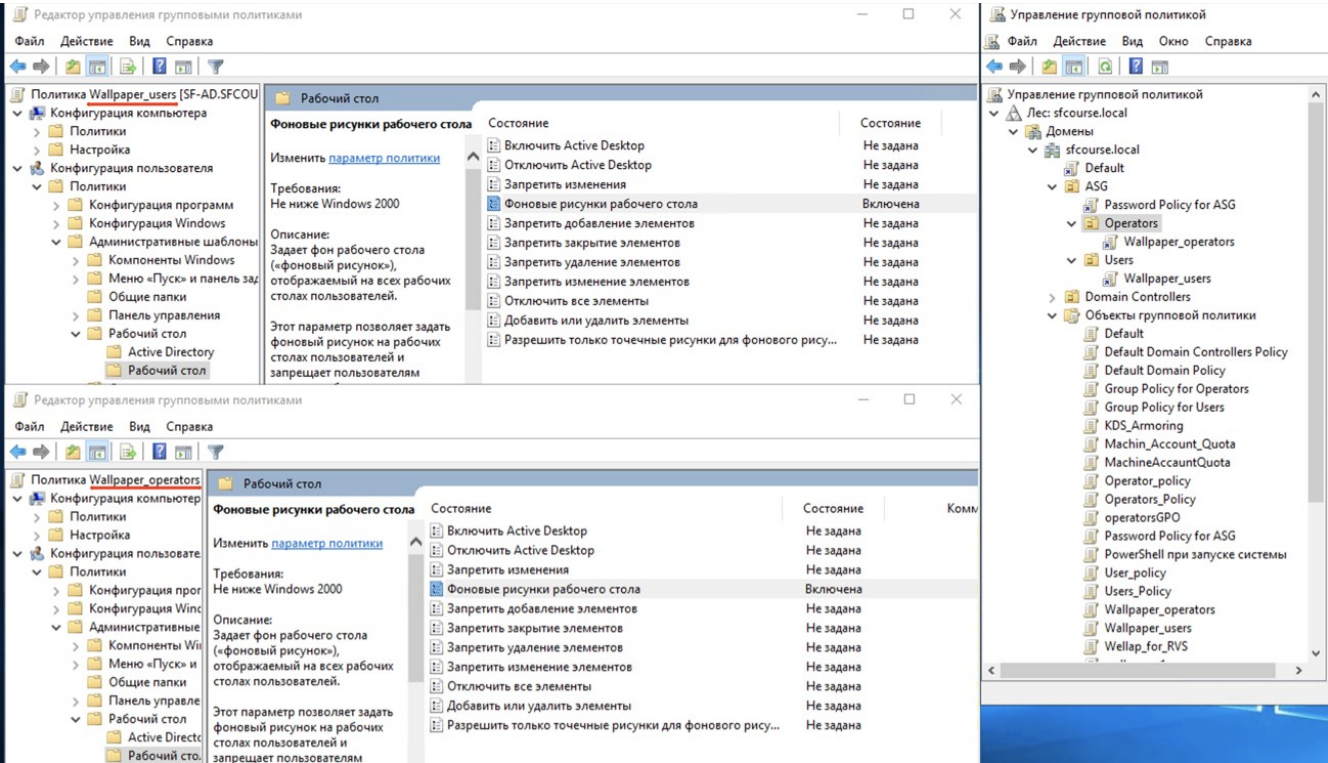


2. Создание групповых политик для двух новых групп.

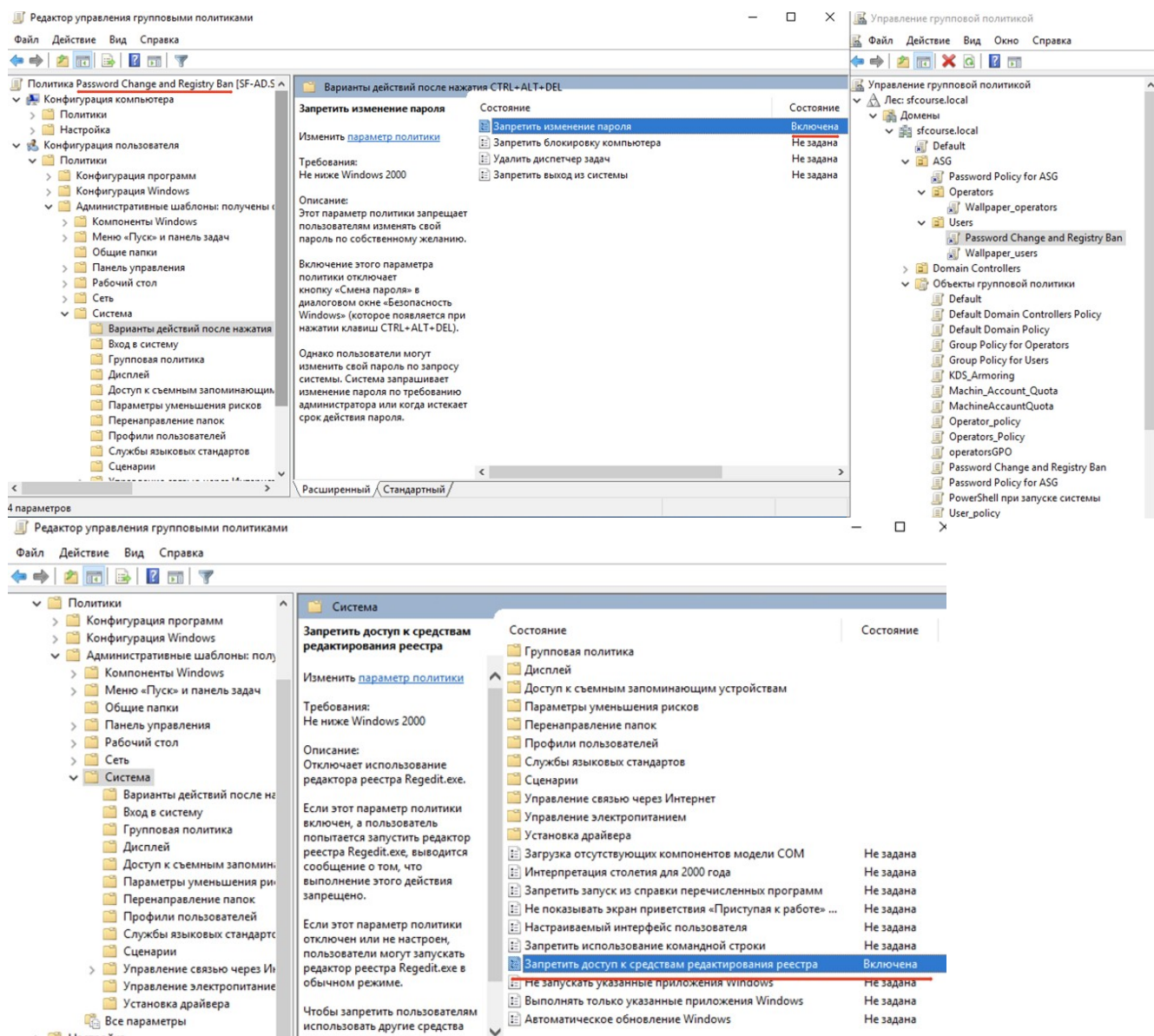
3-5. Настройка групповой политики паролей для Operators и Users.



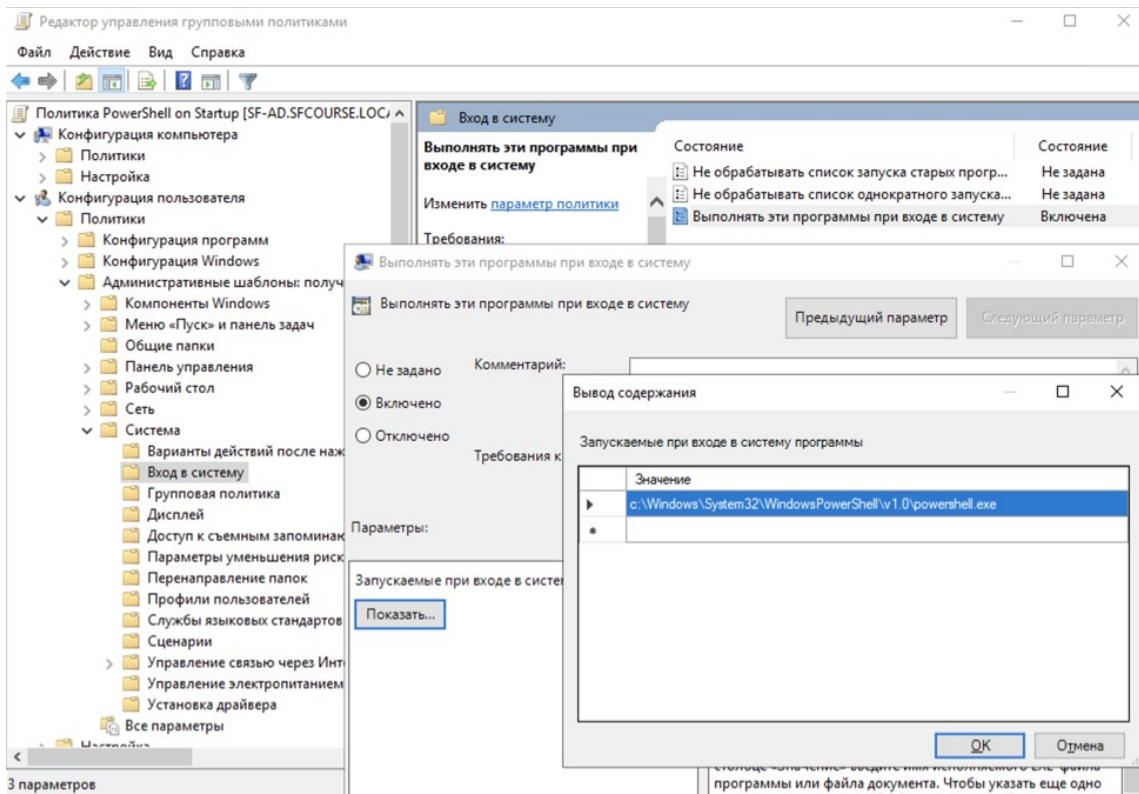
Настройка политики фона рабочего стола для Users и Operators.



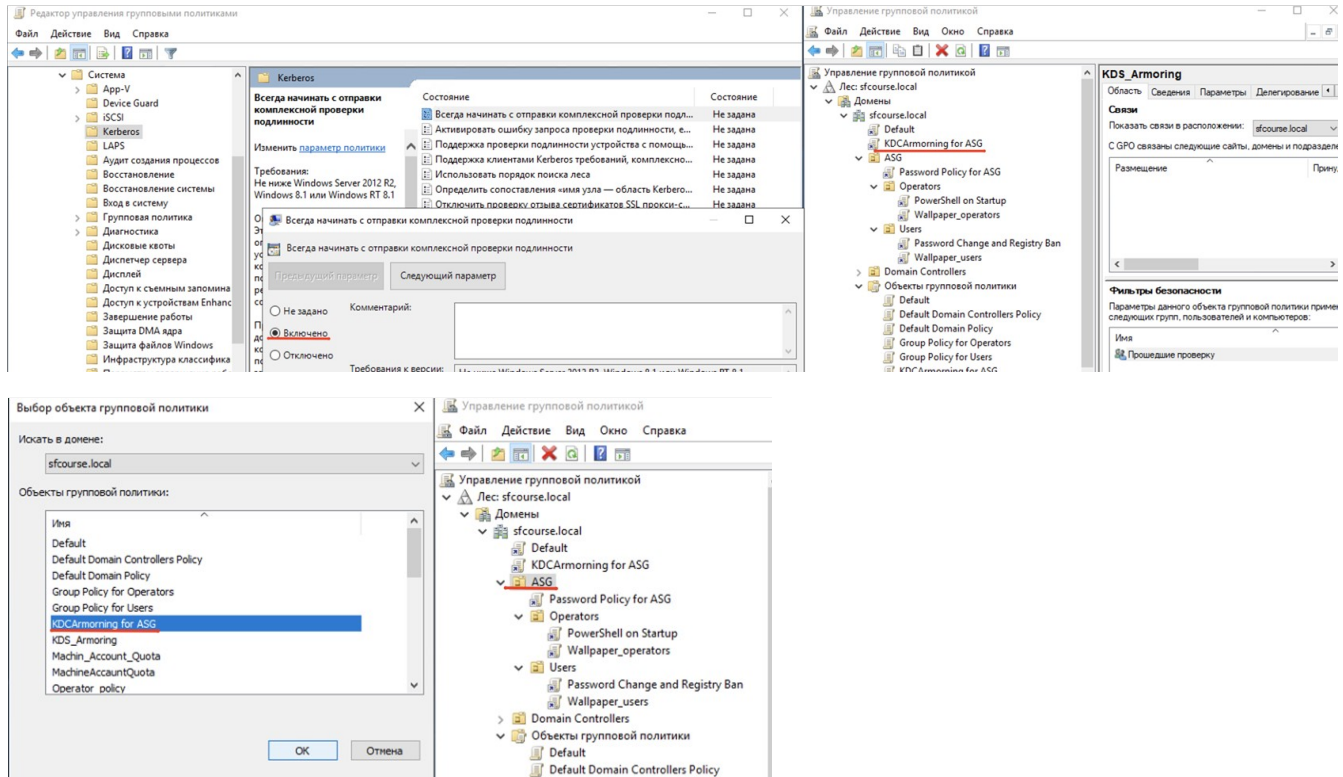
Запрет на изменение пароля для Users.



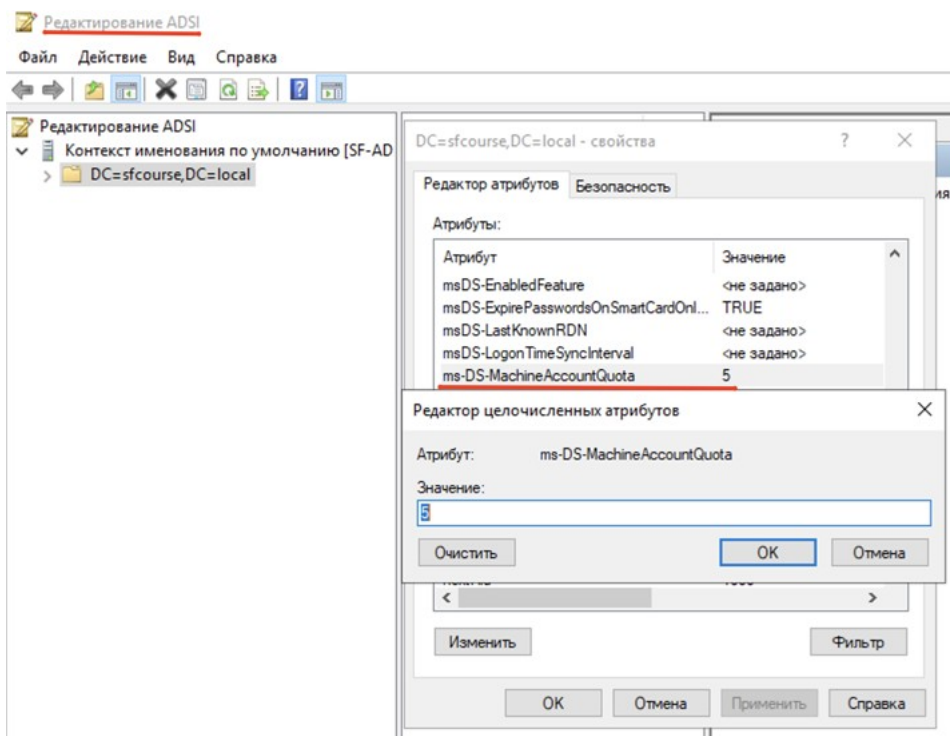
Настройка автозапуска MS PowerShell при входе в систему пользователей группы Operators.



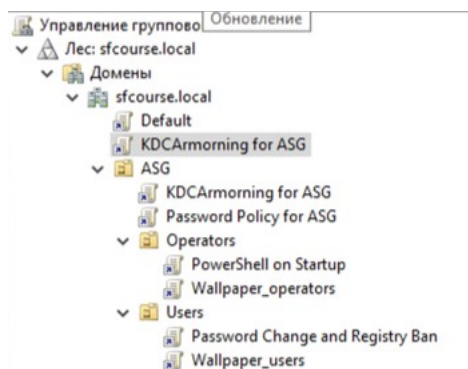
6. Включение KDC Armoring.



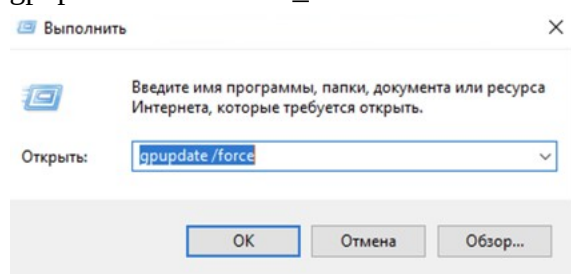
Настройка ms-MachineAccountQuota.



Список политик ASG.



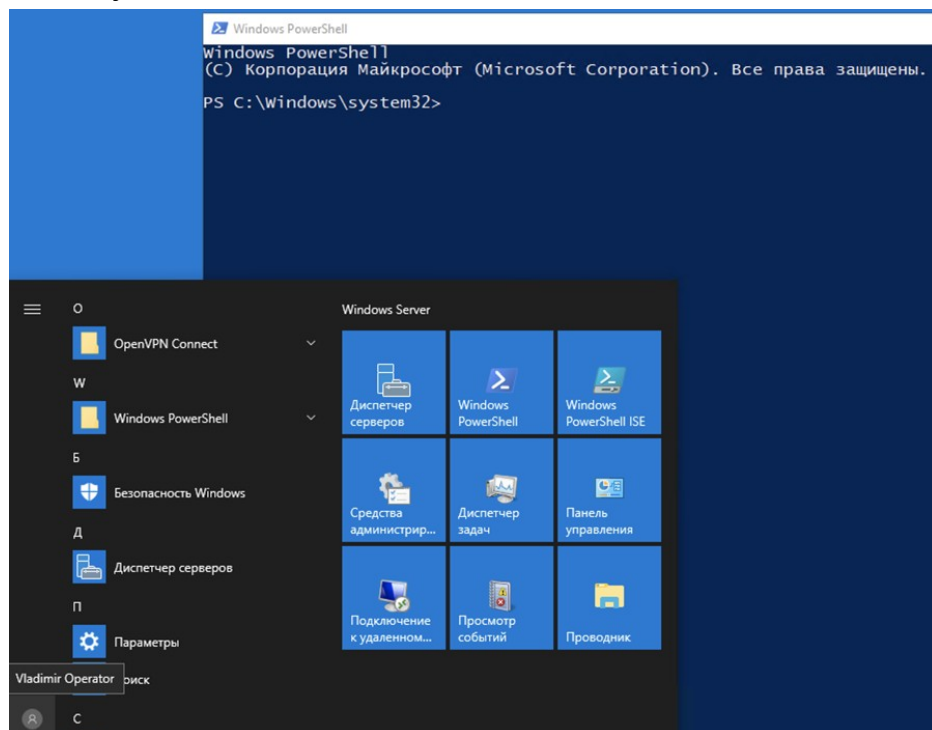
gpupdate /force on SF_CLIENT.



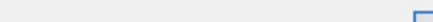
Скриншоты входа на SF_CLIENT под доменными пользователями с разными ролями.

Operators: aoperator

Автозапуск PowerShell:



The screenshot shows the Windows 10 Start menu interface. On the left, a vertical list of apps includes 'OpenVPN Connect', 'Windows PowerShell', 'Безопасность Windows', 'Диспетчер серверов', and 'Параметры'. Below this list, the user profile 'Svetlana User' and a search bar are visible. The main area of the Start menu displays a grid of app tiles for 'Диспетчер серверов', 'Windows PowerShell', 'Windows PowerShell ISE', 'Средства администрир...', 'Диспетчер задач', 'Панель управления', 'Подключение к удаленном...', 'Просмотр событий', and 'Проводник'. The taskbar at the bottom shows the 'Svetlana User' profile and a search bar.



CN=Administrator,CN=Users,DC=sfcourse,DC=local

Последнее применение групповой политики: 06.06.2023 в 11:50:03
Групповая политика была применена с: SF-AD.sfcourse.local
Порог медленного канала для групповой политики: 500 kbps
Имя домена: SFCOURSE
Тип домена: Windows 2008 или более поздняя версия

Примененные объекты групповой политики

Н/Д

Следующие политики GPO не были применены, так как они отфильтрованы

Local Group Policy

Фильтрация: Не применяется (пусто)

Пользователь является членом следующих групп безопасности

Пользователи домена

Все

Администраторы

Пользователи

Пред-Windows 2000 доступ

REMOTE INTERACTIVE LOGON

ИНТЕРАКТИВНЫЕ

Прошедшие проверку

Данная организация

ЛОКАЛЬНЫЕ

Владельцы-создатели групповой политики

Администраторы домена

Администраторы предприятия

Администраторы схемы

Подтвержденное центром проверки подлинности удостоверение

Группа с запрещением репликации паролей RODC

Высокий обязательный уровень

Привилегии безопасности данного пользователя

Обход перекрестной проверки

Управление аудитом и журналом безопасности

Архивация файлов и каталогов

Восстановление файлов и каталогов

Изменение системного времени

Завершение работы системы

Принудительное удаленное завершение работы

Смена владельцев файлов и других объектов

Отладка программ

Изменение параметров среды изготовителя

Профилирование производительности системы

Профилирование одного процесса
Увеличение приоритета выполнения
Загрузка и выгрузка драйверов устройств
Создание файла подкачки
Настройка квот памяти для процесса
Отключение компьютера от стыковочного узла
Выполнение задач по обслуживанию томов
Имитация клиента после проверки подлинности
Создание глобальных объектов
Изменение часового пояса
Создание символических ссылок
Получить маркер олицетворения для другого пользователя в том же сеансе
Разрешение доверия к учетным записям компьютеров и пользователей при делегировании
Увеличение рабочего набора процесса
Добавление рабочих станций к домену

Результирующий набор политик для пользователя

Установка программ

Н/Д

Сценарии входа

Н/Д

Сценарии выхода

Н/Д

Политики открытого ключа

Н/Д

Административные шаблоны

Н/Д

Перенаправление папок

Н/Д

Пользовательский интерфейс браузера Internet Explorer

Н/Д

Подключения Internet Explorer

Н/Д

URL-адреса Internet Explorer

Н/Д

Безопасность Internet Explorer

Н/Д

Программы Internet Explorer

Н/Д

Вывод gpresult /scope computer.

PS C:\Users\Администратор> gpresult /scope COMPUTER /Z

Программа формирования отчета групповой политики операционной системы

Microsoft (R) Windows (R) версии 2.0

© Корпорация Майкрософт (Microsoft Corporation), 2018. Все права защищены.

Создано 06.06.2023 в 13:40:22

Данные RSOP для на SF-AD : Режим ведения журнала

Конфигурация ОС: Основной контроллер домена

Версия ОС: 10.0.17763

Имя сайта: Default-First-Site-Name

Перемещаемый профиль:

Локальный профиль:

Подключение по медленному каналу: Нет

Конфигурация компьютера

CN=SF-AD,OU=Domain Controllers,DC=sfcourse,DC=local

Последнее применение групповой политики: 06.06.2023 в 13:35:54

Групповая политика была применена с: SF-AD.sfcourse.local

Порог медленного канала для групповой политики: 500 kbps

Имя домена: SFCOURSE

Тип домена: Windows 2008 или более поздняя версия

Примененные объекты групповой политики

Default Domain Controllers Policy

KDCArmoring for ASG

Следующие политики GPO не были применены, так как они отфильтрованы

Local Group Policy

Фильтрация: Не применяется (пусто)

Компьютер является членом следующих групп безопасности

Администраторы

Все

Пред-Windows 2000 доступ

Пользователи

Группа авторизации доступа Windows

СЕТЬ

Прошедшие проверку

Данная организация

SF-AD\$

Контроллеры домена

КОНТРОЛЛЕРЫ ДОМЕНА ПРЕДПРИЯТИЯ

Подтвержденное центром проверки подлинности удостоверение

Группа с запрещением репликации паролей RODC

Обязательный уровень системы

Результирующий набор политик для компьютера

Установка программ

Н/Д

Сценарии запуска

Н/Д

Сценарии завершения работы

Н/Д

Политики учетных записей

Н/Д

Политика аудита

Н/Д

Права пользователя

GPO: Default Domain Controllers Policy

Политика: MachineAccountPrivilege
Параметры компьютера: Прошедшие проверку

GPO: Default Domain Controllers Policy

Политика: ChangeNotifyPrivilege
Параметры компьютера: Все
LOCAL SERVICE
NETWORK SERVICE
Администраторы
Прошедшие проверку
Пред-Windows 2000 доступ

GPO: Default Domain Controllers Policy

Политика: IncreaseBasePriorityPrivilege
Параметры компьютера: Администраторы
Window Manager\Window Manager Group

GPO: Default Domain Controllers Policy

Политика: TakeOwnershipPrivilege
Параметры компьютера: Администраторы

GPO: Default Domain Controllers Policy

Политика: RestorePrivilege
Параметры компьютера: Администраторы
Операторы архива
Операторы сервера

GPO: Default Domain Controllers Policy

Политика: DebugPrivilege
Параметры компьютера: Администраторы

GPO: Default Domain Controllers Policy

Политика: SystemTimePrivilege
Параметры компьютера: LOCAL SERVICE
Администраторы
Операторы сервера

GPO: Default Domain Controllers Policy

Политика: SecurityPrivilege
Параметры компьютера: Администраторы

GPO: Default Domain Controllers Policy

Политика: ShutdownPrivilege
Параметры компьютера: Администраторы
Операторы архива
Операторы сервера
Операторы печати

GPO: Default Domain Controllers Policy

Политика: AuditPrivilege
Параметры компьютера: LOCAL SERVICE
NETWORK SERVICE

GPO: Default Domain Controllers Policy

Политика: InteractiveLogonRight
Параметры компьютера: Администраторы
Операторы архива
Операторы учета
Операторы сервера
Операторы печати
КОНТРОЛЛЕРЫ ДОМЕНА ПРЕДПРИЯТИЯ

GPO: Default Domain Controllers Policy

Политика: CreatePagefilePrivilege
Параметры компьютера: Администраторы

GPO: Default Domain Controllers Policy

Политика: BatchLogonRight
Параметры компьютера: Администраторы
Операторы архива
Пользователи журналов производительности

GPO: Default Domain Controllers Policy

Политика: NetworkLogonRight
Параметры компьютера: Все
Администраторы
Прошедшие проверку
КОНТРОЛЛЕРЫ ДОМЕНА ПРЕДПРИЯТИЯ
Пред-Windows 2000 доступ

GPO: Default Domain Controllers Policy

Политика: SystemProfilePrivilege
Параметры компьютера: Администраторы
NT SERVICE\WdiServiceHost

GPO: Default Domain Controllers Policy

Политика: RemoteShutdownPrivilege
Параметры компьютера: Администраторы
Операторы сервера

GPO: Default Domain Controllers Policy

Политика: BackupPrivilege
Параметры компьютера: Администраторы
Операторы архива
Операторы сервера

GPO: Default Domain Controllers Policy

Политика: EnableDelegationPrivilege

Параметры компьютера: Администраторы

GPO: Default Domain Controllers Policy

Политика: UndockPrivilege

Параметры компьютера: Администраторы

GPO: Default Domain Controllers Policy

Политика: SystemEnvironmentPrivilege

Параметры компьютера: Администраторы

GPO: Default Domain Controllers Policy

Политика: LoadDriverPrivilege

Параметры компьютера: Администраторы

Операторы печати

GPO: Default Domain Controllers Policy

Политика: IncreaseQuotaPrivilege

Параметры компьютера: LOCAL SERVICE

NETWORK SERVICE

Администраторы

GPO: Default Domain Controllers Policy

Политика: ProfileSingleProcessPrivilege

Параметры компьютера: Администраторы

GPO: Default Domain Controllers Policy

Политика: AssignPrimaryTokenPrivilege

Параметры компьютера: LOCAL SERVICE

NETWORK SERVICE

Параметры безопасности

Н/Д

GPO: Default Domain Controllers Policy

Политика: @wsecedit.dll,-59013

Параметр: MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\
LDAPServerIntegrity

Параметры компьютера: 1

GPO: Default Domain Controllers Policy

Политика: @wsecedit.dll,-59043

Параметр: MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\
RequireSecuritySignature

Параметры компьютера: 1

GPO: Default Domain Controllers Policy

Политика: @wsecedit.dll,-59044

Параметр: MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\
EnableSecuritySignature
Параметры компьютера: 1

GPO: Default Domain Controllers Policy
Политика: @wsecedit.dll,-59018
Параметр: MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\
RequireSignOrSeal
Параметры компьютера: 1

Параметры журнала событий

Н/Д

Группы с ограниченным доступом

Н/Д

Системные службы

Н/Д

Параметры реестра

Н/Д

Параметры файловой системы

Н/Д

Политики открытого ключа

Н/Д

Административные шаблоны

GPO: KDCArmoring for ASG
Идентификатор папки: Software\Microsoft\Windows\CurrentVersion\Policies\System\
Kerberos\Parameters\AlwaysSendCompoundId
Значение: 1, 0, 0, 0
Состояние: Включено