

2023



Master UTM

Инструкция по настройке удаленного подключения через технологию [WMI](#) (Windows Management Instrumentation) .



В данной инструкции описывается процесс по настройке удаленного подключения через технологию WMI (Windows Management Instrumentation).

Внимание! Работы по настройке должны выполнять специалисты соответствующей квалификации – системный администратор или администратор баз данных. Если вы не уверены в своих силах, то можете заказать услугу по настройке на сайте нашей компании <https://egais.center-inform.ru>.

Техническая поддержка по работе программы «Master UTM» осуществляется на портале по адресу <http://support.center-inform.ru>.

Внимание! Весь процесс настройки необходимо выполнять с правами администратора или под учетной записью администратора на данном ПК.

Если вышеуказанные условия выполнены, то перейдем к последовательному выполнению обязательных операций:

1. Разрешение DCOM;
2. Разрешение пользователю на доступ к пространству имен WMI;
3. Проверка прав на олицетворение WMI

1. Разрешение DCOM

Вызовите командную строку, запустите её от имени администратора. Наберите команду Dcomcnfg и нажмите Enter. Откроется окно “Службы компонентов”. Разверните службу компонентов -> Компьютеры -> Мой компьютер.

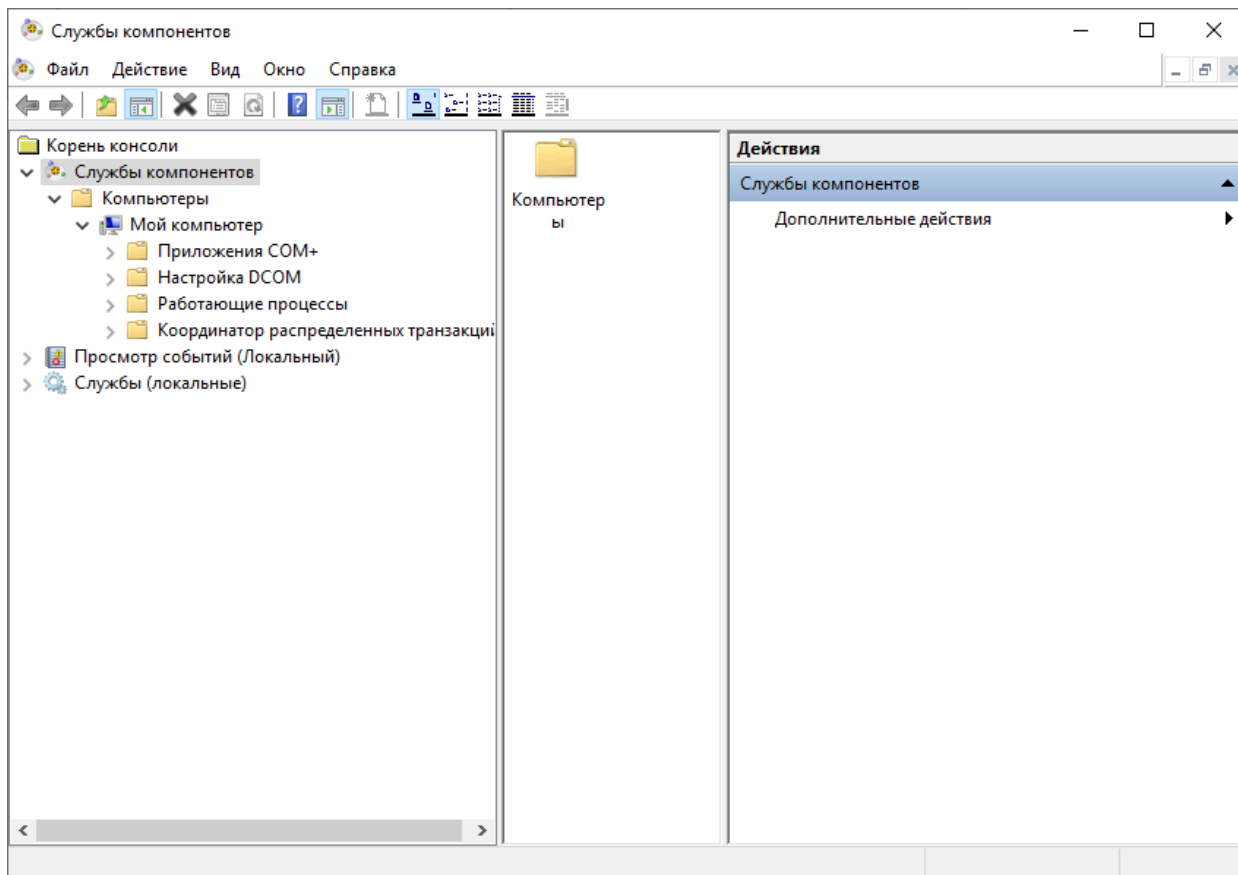


Рис. 1. Службы компонентов.

Перейдите в свойства “Мой компьютер “. Выберите вкладку Безопасность COM. Нажмите "Изменить ограничения" в разделе "Права доступа" и убедитесь, что у группы пользователей "Все" есть разрешения "Локальный доступ" и "Удаленный доступ". Нажмите на "Редактировать ограничение" для разрешений на запуск и активацию и убедитесь, что у группы пользователей "Все" есть разрешения "Локальная активация" и "Локальный запуск".

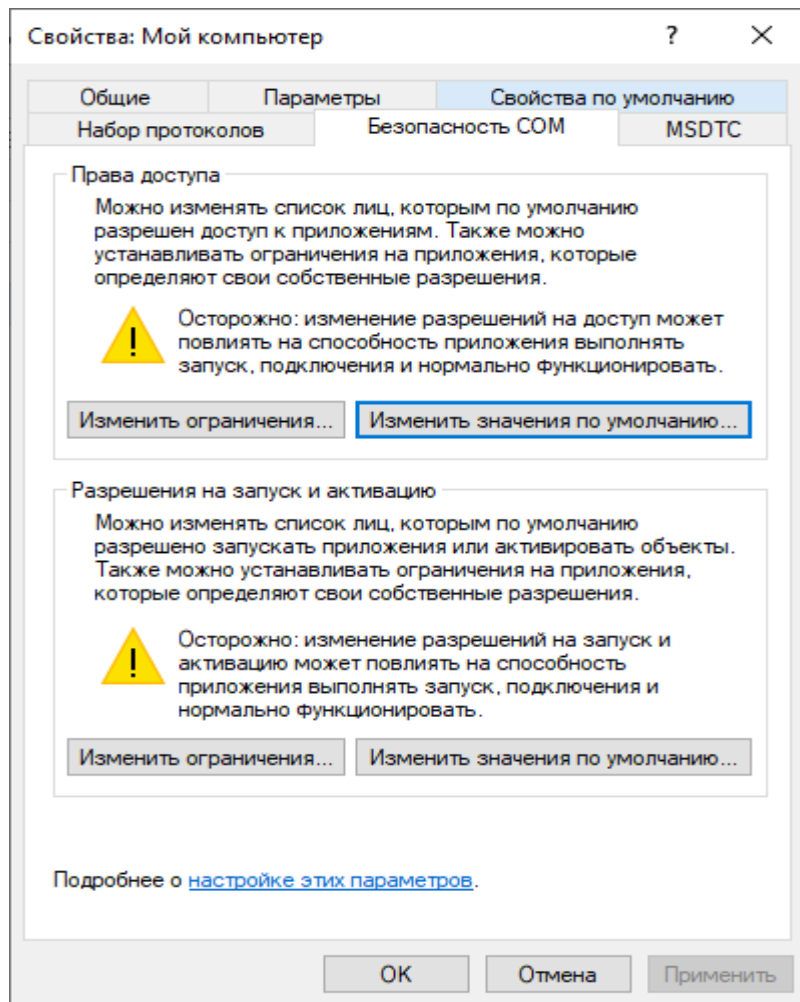


Рис. 2 Свойства Мой компьютер.

Выделите узел "Настройка DCOM", щелкните правой кнопкой мыши на значке "Управление Windows и инструменты" (Windows Management and Instrumentation) и выберите "Свойства".

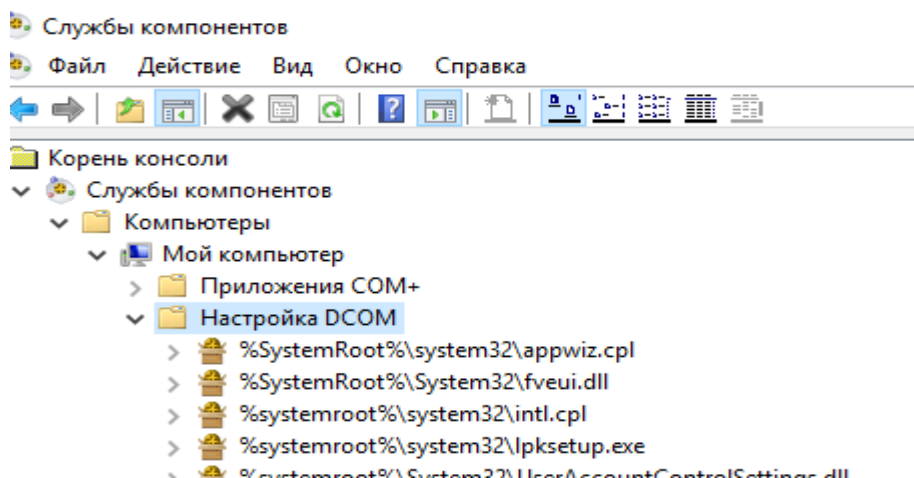


Рис. 3. Узел Настройка DCOM.

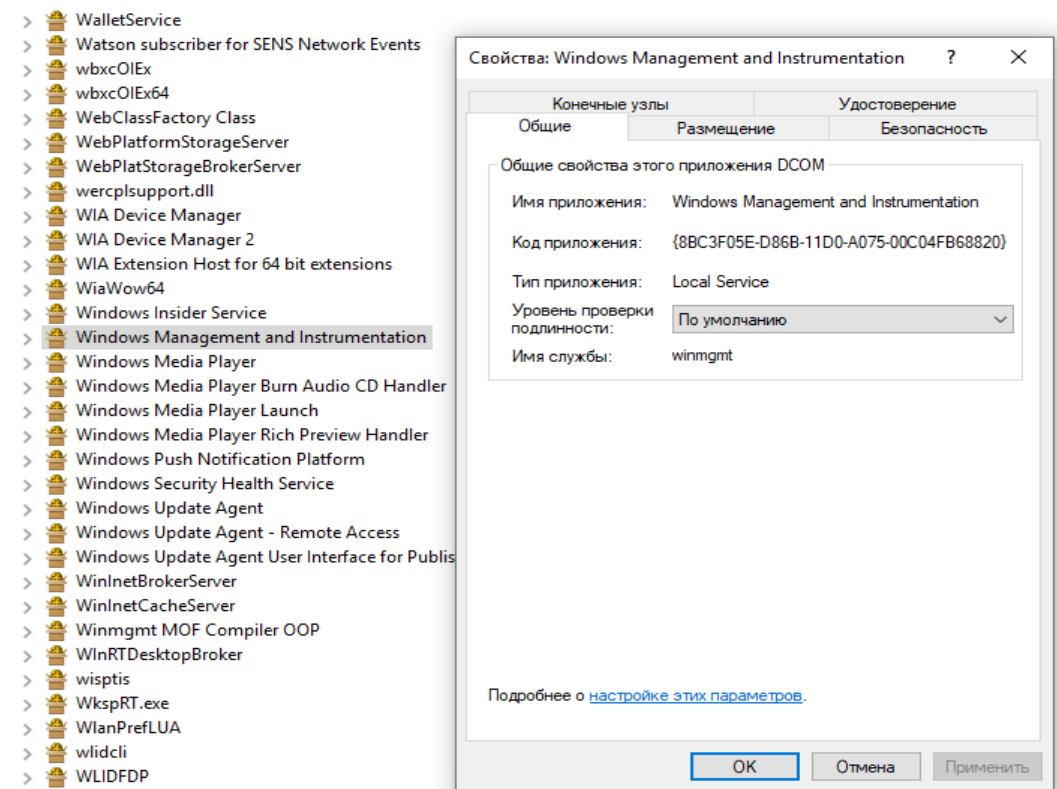


Рис. 4. Выбор "Управление Windows и инструменты".

В разделе безопасность добавьте все права в трех разделах («Разрешения на запуск и активацию», «Разрешение на доступ», «Разрешение на изменение настроек») для Администраторы и «Прошедшие проверку»:

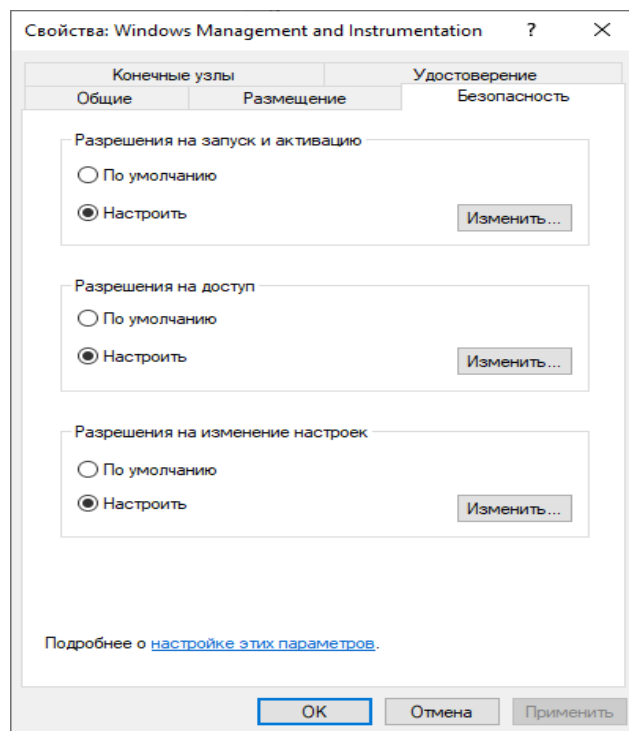


Рис.5. Свойства Windows Management and Instrumentation.

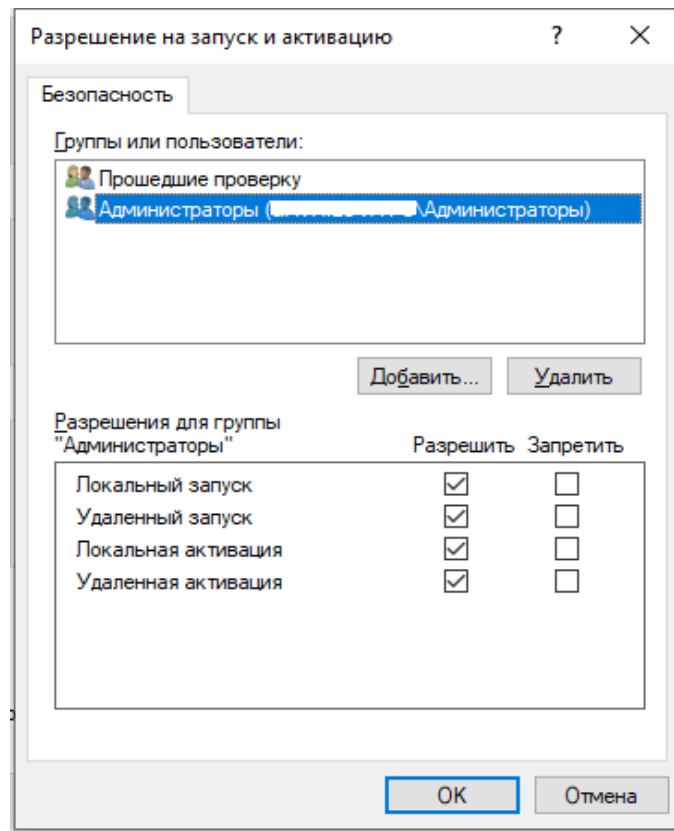


Рис. 6. Разрешение на запуск и активацию.

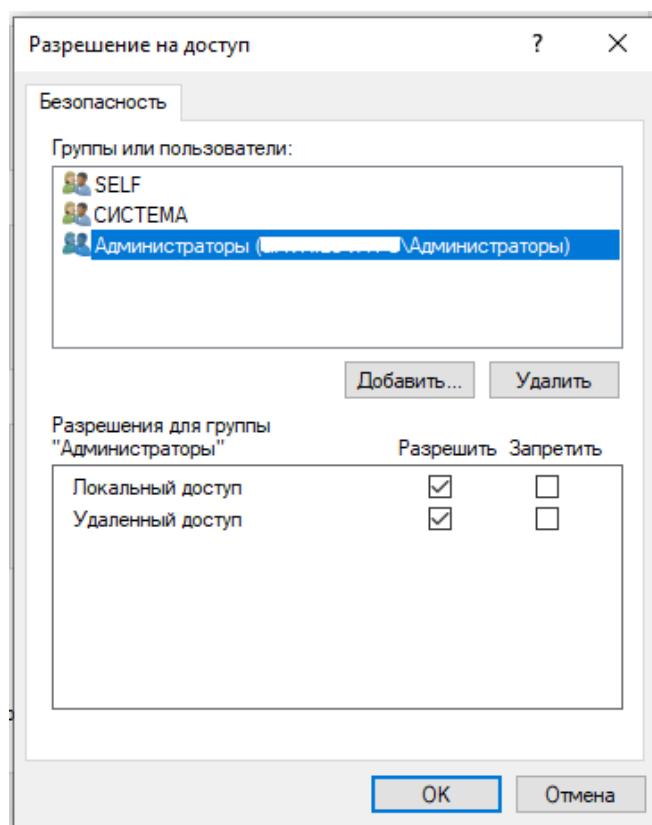


Рис. 7. Разрешение на доступ.

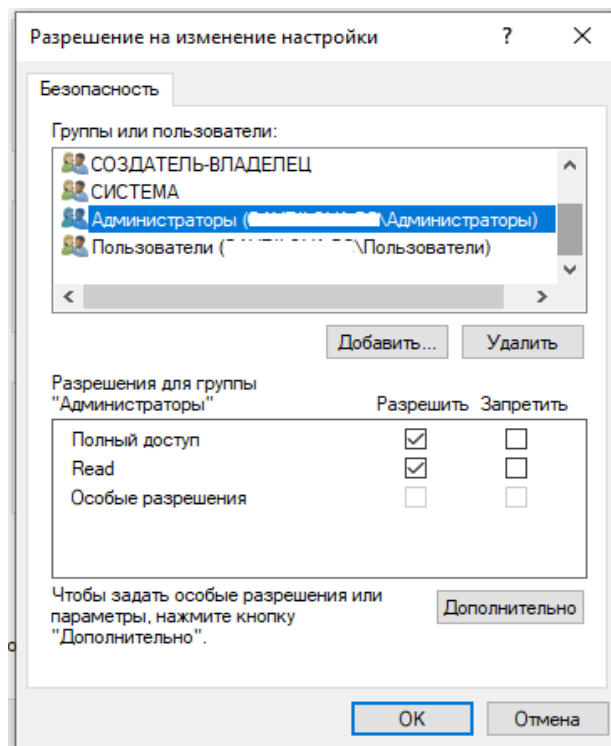


Рис. 8 Разрешение на изменение настройки.

2. Разрешение пользователю на доступ к пространству имен WMI

Откройте через командную строку WMImgmt.msc. Перейдите к свойствам элемента управления WMI. Перейдите на вкладку Безопасность.

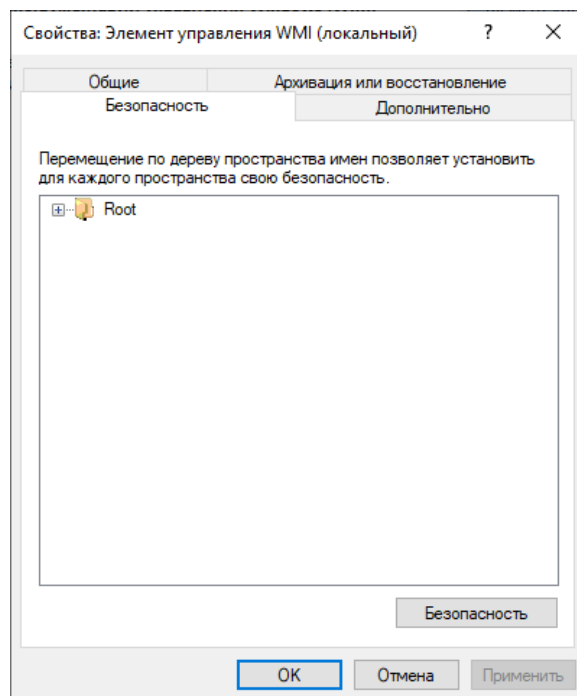


Рис. 9. Свойства Элемента управления WMI (локальный)

Выберите "Root" и откройте "Безопасность". Убедитесь, что у "аутентифицированных пользователей" есть права "Выполнять методы", "Права поставщика" и "Включить учетную запись"; убедитесь, что у администраторов есть все разрешения.

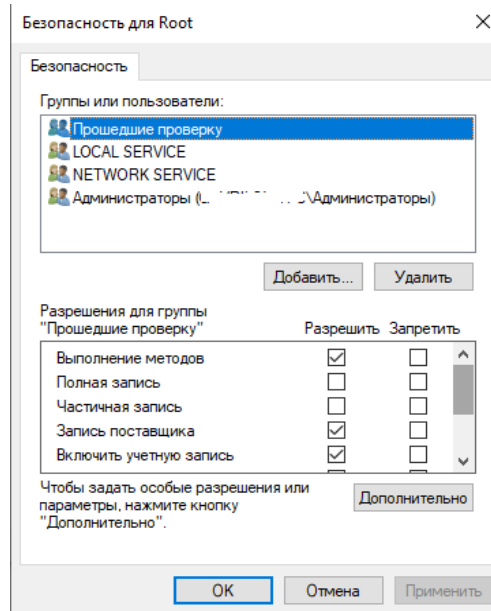


Рис. 10. Проверка безопасности.

3. Проверка прав на олицетворение WMI.

В командной строке введите `gpedit.msc`, нажмите "OK". В разделе Конфигурация Компьютера->Конфигурация Windows -> «Параметры безопасности» -> «Локальные политики», а затем щелкните Назначение прав пользователя.

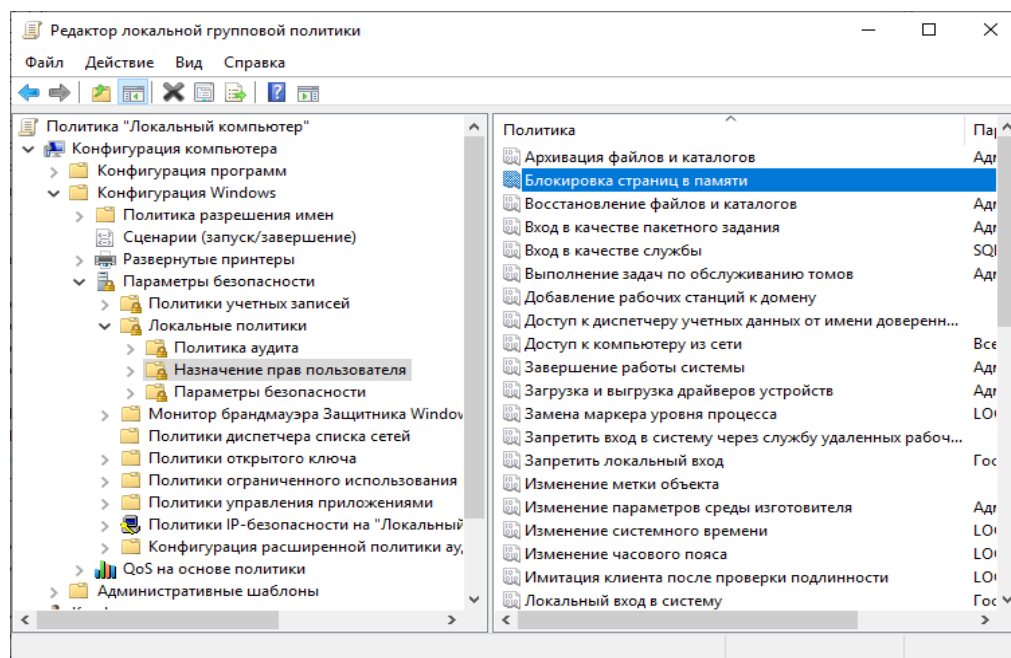


Рис. 11. Редактор локальной групповой политики.

Убедитесь, что учетной записи «СЛУЖБА» предоставлены права выдавать себя за клиента после проверки подлинности (Имитация клиента после проверки подлинности). Найдите для этого в правом списке запись “Имитация клиента после проверки подлинности”, правой кнопкой мыши вызовите свойства.

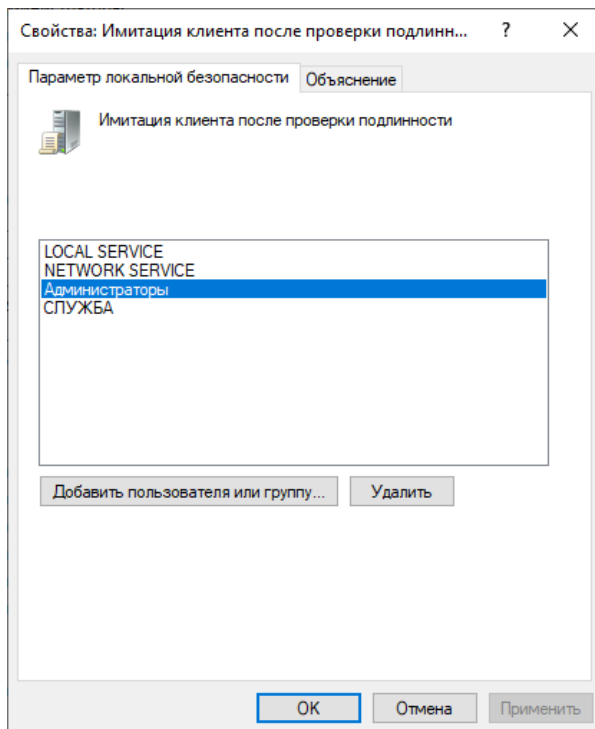


Рис. 12. Имитация клиента после проверки подлинности

Для доступа по WMI необходимо отключить удаленный контроль учетных записей. Откройте редактор реестра (в командной строке наберите команду regedit). Перейдите на ветку <HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system>. Создайте параметр LocalAccountTokenFilterPolicy типа DWORD и пропишите значение равным "1".

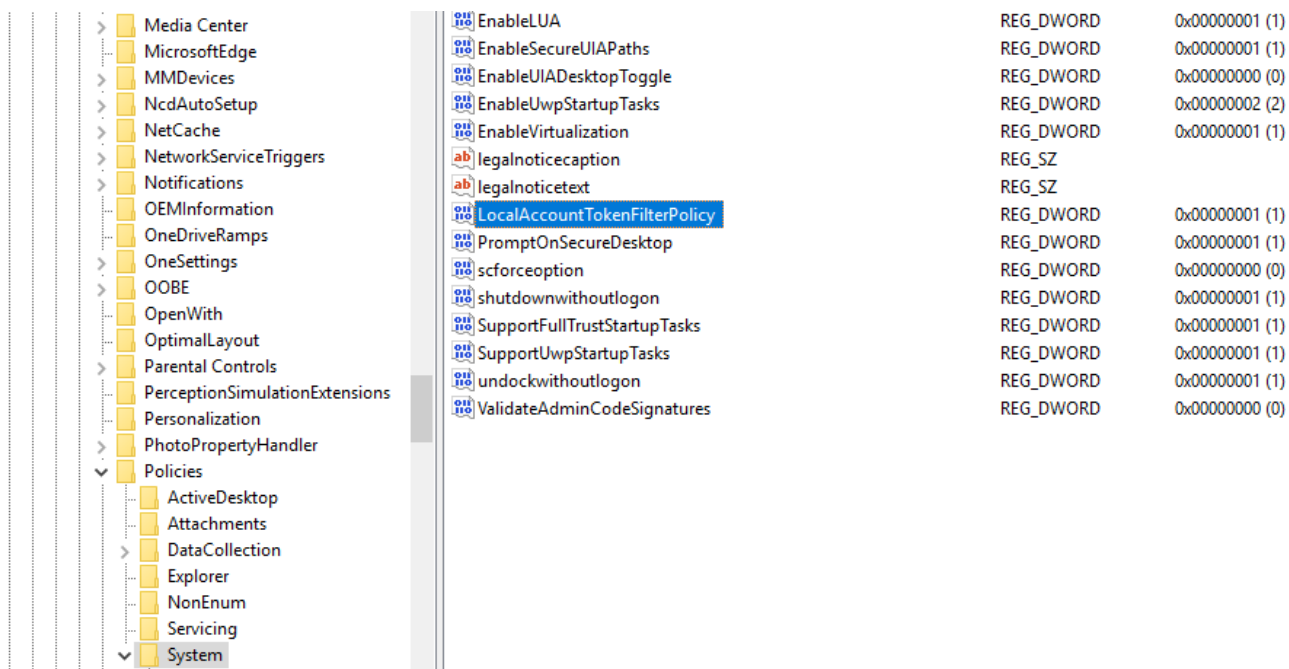


Рис.13. Создание параметра LocalAccountTokenFilterPolicy.

Для компьютеров не из домена, между которыми нет доверительных отношений, потребуется изменить в реестре значение DWORD параметра:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\AllowAnonymousCallback;

0 - запрет обратных вызовов;

1 - разрешает обратные вызовы. Нужно установить значение равное "1".

После внесения изменений в реестр требуется перезагрузка ПК.