Предоставление прав на удаленное подключение к Service Control Manager

http://winitpro.ru/index.php/2016/06/15/predostavlenie-prav-na-udalennoe-podklyuchenie-k-service-control-manager/

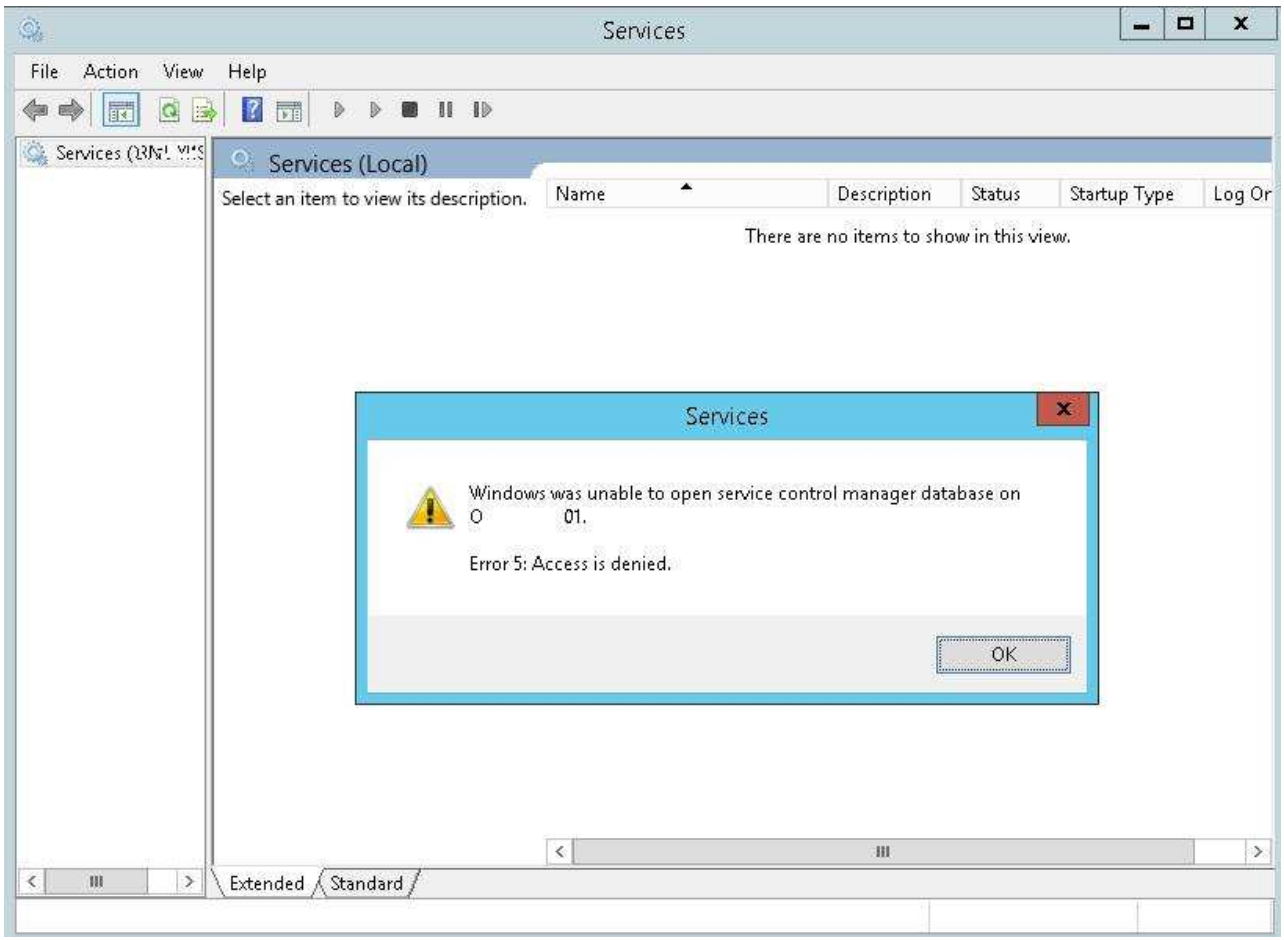
Рассмотрим особенности предоставления прав удаленного доступа к списку служб, запущенных на сервере, доменным пользователем, у которых отсутствуют права локальных администраторов. По сути задача сводится к предоставлению **доступа на удаленное подключение** к интерфейсу диспетчера управления службами — **Service Control Manager** (**SCManager**).

Как выглядит проблема. Допустим, мы хотим, чтобы удаленный пользователь / или система мониторинга могли опрашивать состояние служб на некоем сервере. По понятным причинам этот удаленный пользователь не имеет прав административных права и права на локальный вход на сервер.

При попытке подключиться и получить список служб на удаленном компьютере с помощью консоли services.msc, пользователь получает ошибку:

Windows was unable to open service control manager database on computer_name

Error 5: Access is denied.



Если же попробовать вывести список служб на удаленном сервере с помощью утилиты sc.exe, ошибка такая:

```
C:\Windows\system32>sc \\obts-01 query
```

[SC] OpenSCManager FAILED 5:
Access is denied.

Возможность получить доступ к списку служб контролируется дескриптором безопасности базы данных Service Control Manager, удаленный доступ к которой для пользователей “Authenticated Users” был ограничен еще в Windows 2003 SP1 (что, в общем-то, логично). Права на удаленный доступ к данной службе есть только у членов группы локальных администраторов.

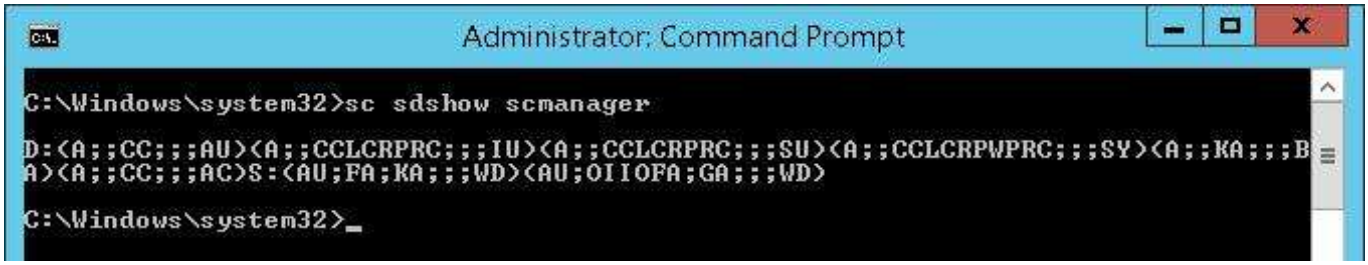
Рассмотрим, как предоставить удаленный доступ к диспетчеру Service Control Manager для получения списка служб сервера и возможность получения их статусов обычным пользователям (без прав администратора) на примере Windows Server 2012 R2.

Текущие разрешения менеджера сервисов (SCM) можно получить с помощью утилиты **sc.exe**, выполнив в командной строке, запущенной с правами администратора:

```
sc sdshow scmanager
```

Команда вернет примерно такую SDDL строку:

```
D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CC;
;;AC)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)
```



В данном случае видно, что по умолчанию группе Authenticated Users (AU) разрешено только подключаться в SCM, но не опрашивать (LC) службы. Скопируйте строку в окно любого тестового редактора.

Следующий этап – получение SID пользователя или группы, которой мы хотим предоставить удаленный доступ к SCM (Как получить SID пользователя по имени). К примеру, получим SID AD группы msk-hd так:

```
Get-ADgroup -Identity 'msk-hd' | select SID

SID
---
S-1-5-21-2470146451-3958456388-2988885117-23703978
```

В текстовом редакторе в SDDL строке нужно скопировать блок **(A;;CCLCRPRC;;;IU)** – (IU – означает Interactive Users)), заменить в скопированном блоке IU на SID пользователя/группы и вставить полученную строку перед **S:**.

В нашем случае получилась такая строка:

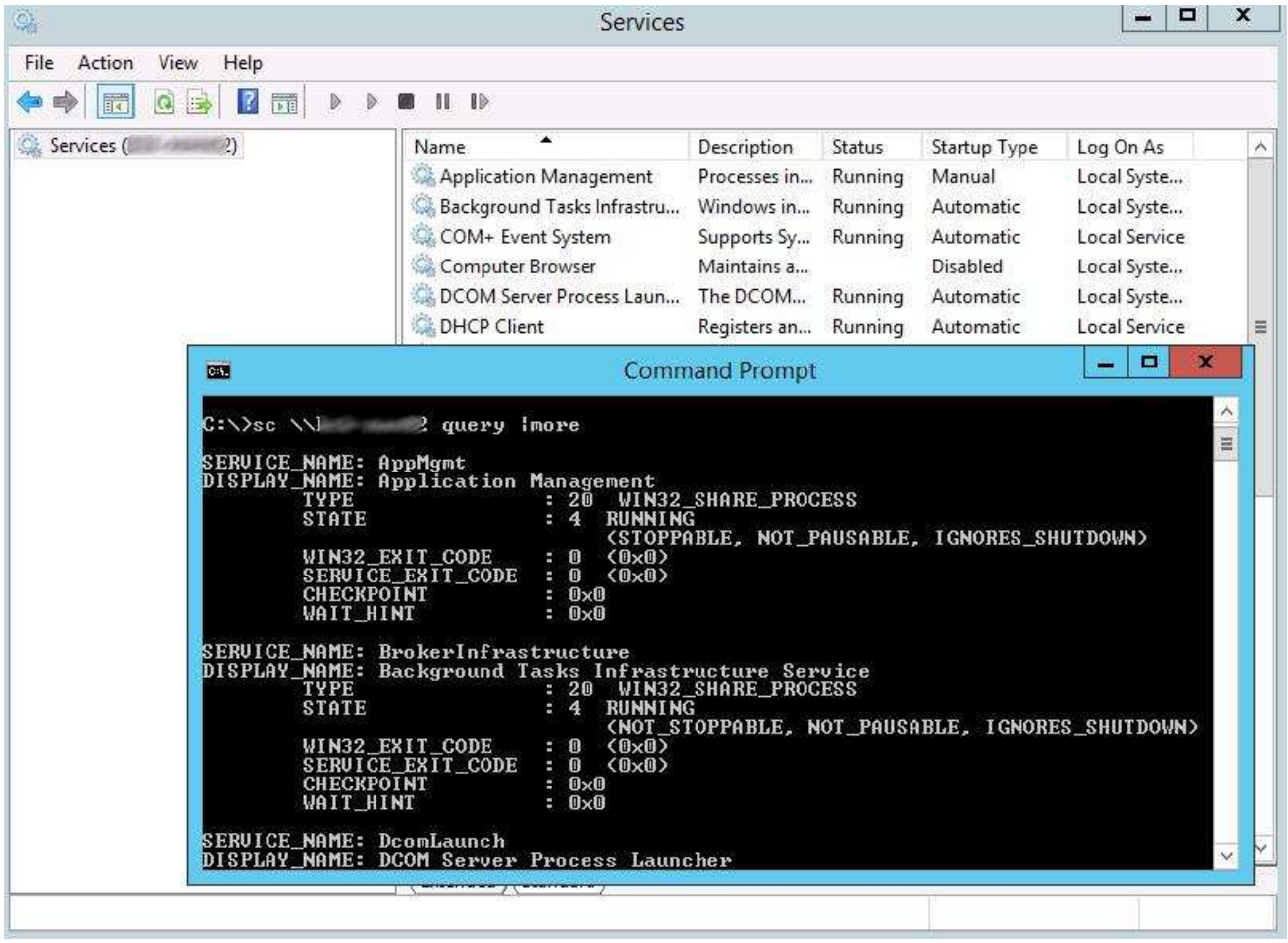
D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CC;;;AC)**(A;;CCLCRPRC;;;*S-1-5-21-2470146451-3958456388-2988885117-23703978*)**S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)

А теперь с помощью sc.exe изменим параметры дескриптора безопасности Service Control Manager:

```
sc sdset scmanager
“D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CC
;;;AC)(A;;CCLCRPRC;;;S-1-5-21-2470146451-3958456388-2988885117-
23703978)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)“
```

Строка *[SC] SetServiceObjectSecurity SUCCESS* говорит о том, что новые параметры безопасности успешно применены, и мы выдали пользователю правам, аналогичные права локально аутентифицированных пользователей: SC_MANAGER_CONNECT, SC_MANAGER_ENUMERATE_SERVICE, SC_MANAGER_QUERY_LOCK_STATUS и STANDARD_RIGHTS_READ.

Проверим, что теперь удаленный пользователь может получать список служб и их статус с помощью консоли управления службами (services.msc) и с помощью запроса sc \\server-name1 query



Права на управление запущенными службами при этом, естественно, отсутствуют, т.к. доступ к каждой службе контролируется индивидуальной ACL. Чтобы предоставить пользователю права на запуск/остановку служб сервера нужно воспользоваться инструкциями из статьи Предоставление прав пользователю на управление (запуск, остановку, перезапуск) службами Windows.

Совет. При назначении прав на SCManager, отличных от стандартных, они сохраняются в ветке HKLM\SYSTEM\CurrentControlSet\Control\ServiceGroupOrder\Security. И если при формировании SDDL строки была допущена ошибка, сбросить текущие разрешения на дефолтные можно простым удалением этой ветки и перезагрузкой.