Прозрачная авторизация на RDS с помощью SSO (Single Sign-On)

19.06.2015 Windows Server 2012 R2 Комментарии (3)

Single Sign-On (**SSO** — технология единого входа) это технология, позволяющая уже аутентифицированному (вошедшему в систему) пользователю получать доступ к другим сервисам без повторной аутентификации. Применительно к технологии терминальных серверов **Remote Desktop Service**, SSO позволяет избавить пользователя, выполнившего вход на доменном компьютере, от многократного ввода данных своей учетной записи при подключении к RDS серверам или запуске опубликованных приложений RemoteApp.

В этой статье мы опишем особенности настройки прозрачной авторизации (Single Sign-On) пользователей на серверах RDS под управлением Windows Server 2012 R2.

Требования к окружению:

- Сервер Connection Broker и все RDS сервера должны работать под управлением Windows Server 2012
- SSO работает только в доменном окружения: должны использоваться учетные записи пользователей Active Directory, а сервера и рабочие станции должны быть в составе домена
- Требуется версия клиента RDP 8.0 и выше
- На стороне клиента поддерживаются OCWindow 7/8/8.1
- SSO работает с парольной аутентификацией (смарт карты не поддерживаются)

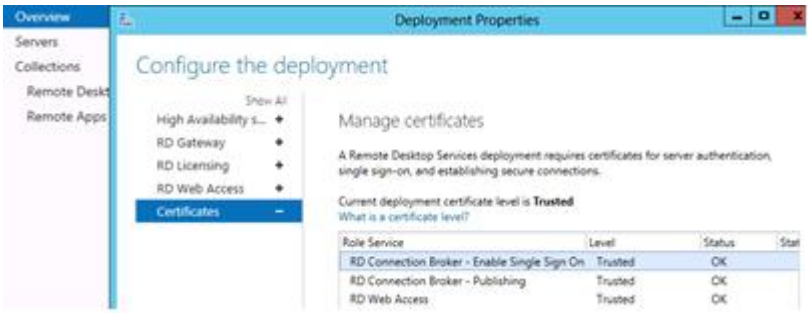
Процедура настройки Single Sign-On состоит из следующих этапов:

- Необходимо выпустить и назначить SSL сертификат на серверах RD Gateway, RD Web и RD Connection Broker

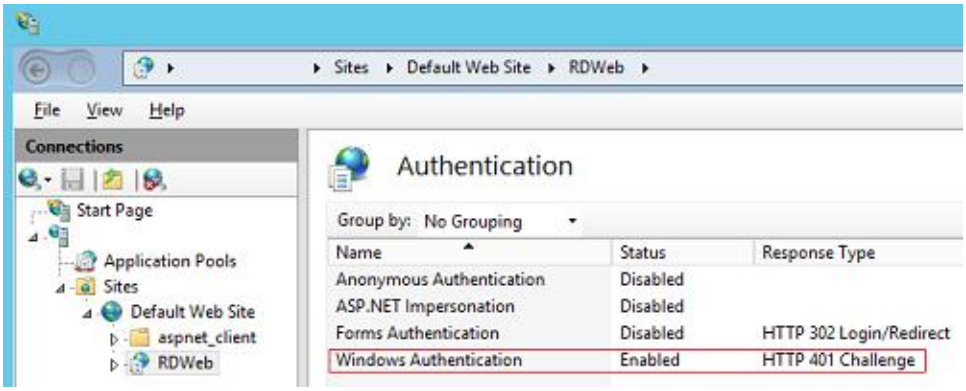
- Включить Web SSO на сервере RDWeb
- Настроить групповую политику делегирования учетных данных
- Через GPO добавить отпечаток сертификата в доверенные издатели .rdp

Итак, в первую очередь нужно выпустить и назначить SSL сертификат (в EKU сертификата должно обязательно присутствовать **Server Authentication**). Мы опускаем процедуру получения сертификата, т.к. это она выходит за рамки статьи.

Сертификат назначается в свойствах **RDS Deployment** в подразделе **Certificates**.



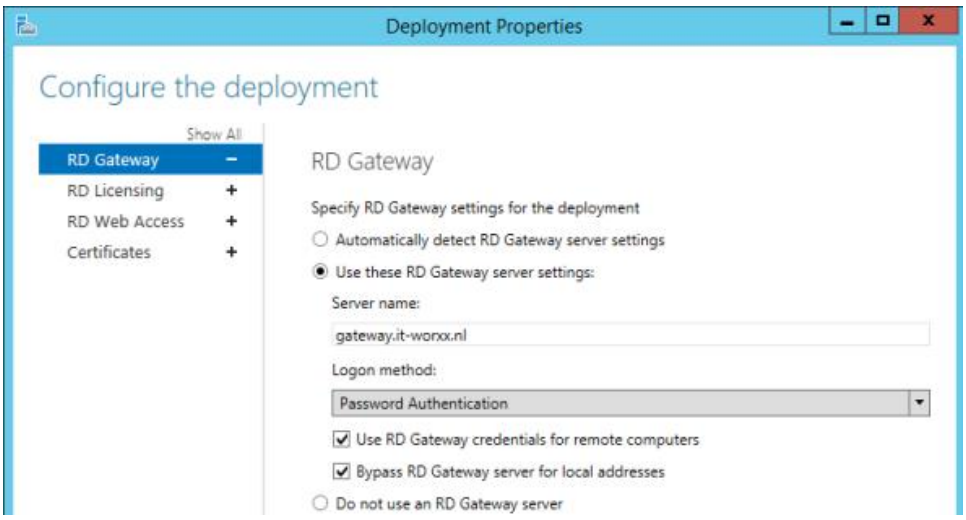
Далее на всех серверах с ролью Web Access для каталога IIS RDWeb нужно включать "**Windows Authentication**" и отключить анонимную проверку подлинности (**Anonymous Authentication**).



После сохранения изменений, IIS нужно перезапустить:

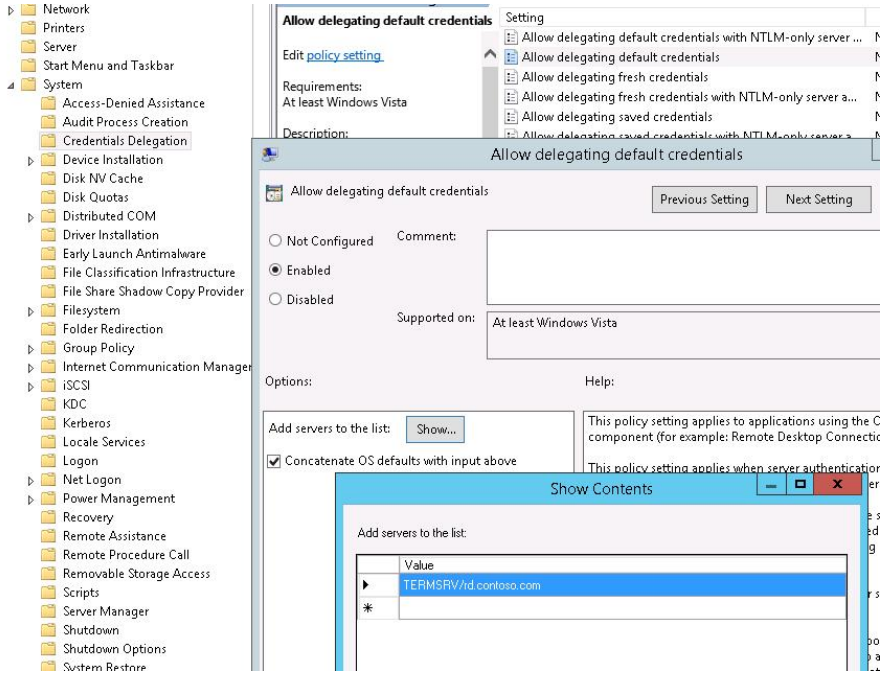
```
iisreset /noforce
```

В том случае, если используется шлюз RD Gateway, убедитесь, что он не используется для подключения внутренних клиентов (должна стоять галка **Bypass RD Gateway server for local address**).



Следующий этап – настройка политики делегирования учетных данных. Эта политика находится в разделе **Computer Configuration -> Policies ->Administrative Templates -> System -> Credential Delegation -> Allow delegation defaults credential**. Политика разрешает определенным серверам доступ к учетным данным пользователей Windows.

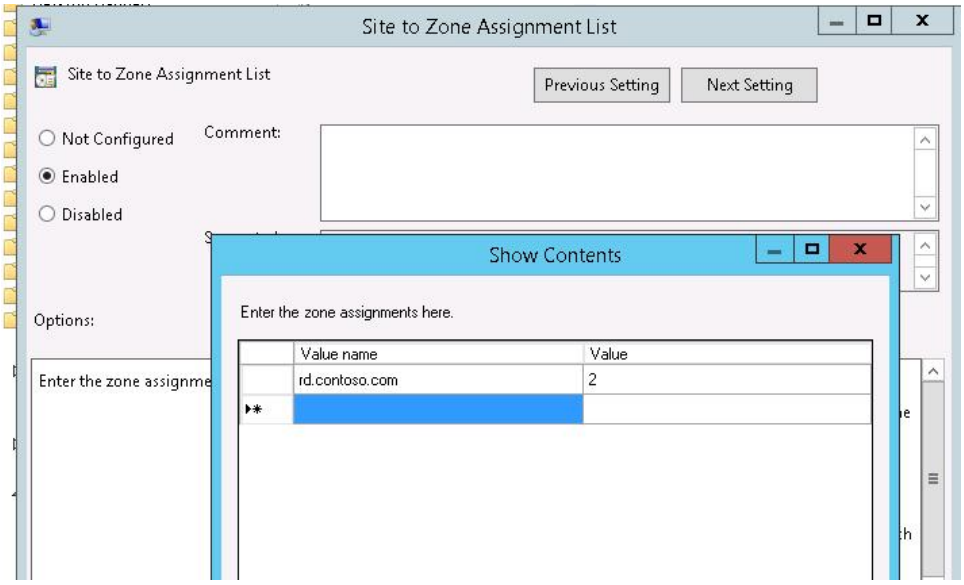
- Политику нужно включить (**Enabled**)
- А в списке серверов добавить имена RDS серверов, на которых происходит авторизация. Формат добавления сервера: **TERMSRV/rd.contoso.com**. Если нужно предоставить такое право всем терминальным системам домена (менее безопасно), можно воспользоваться такой конструкцией: TERMSRV/*.contoso.com



Далее, чтобы избежать появления окна с предупреждением о надежности издателя удаленного приложения, нужно с помощью GPO на клиентских компьютерах добавить адрес сервера с ролью Connection Broker в доверенную зону:

User/Computer Configuration -> Administrative Tools -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page-> Site to Zone assignment list

Указываем **FQDN** имя сервера RDCB и зону **2** (Trusted sites)

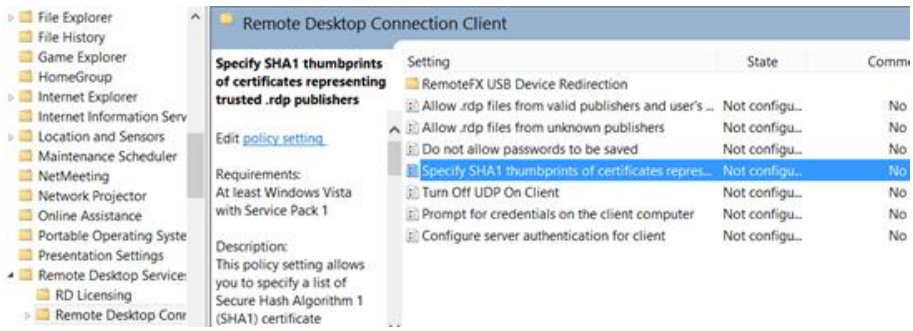


Далее нужно включить политику **Logon options** в разделе **User/Computer Configuration -> Administrative Tools -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security -> Trusted Sites Zone** и в выпадающем списке выбрать `**Automatic logon with current username and password**`.

И, последнее, нужно получить отпечаток сертификата (certificate thumbprint) и добавить его в список доверенных издателей rdp. Для этого на сервере RDS Connection Broker выполните команду PowerShell:

```
Get-Childitem CERT:\LocalMachine\My
```

Скопируйте значение отпечатка сертификата и добавьте его в список отпечатков политики **Specify SHA1 thumbprints of certificates representing RDP publishers** (Computer Configuration -> Administrative Templates -> Windows Desktop Services -> Remote Desktop Connection Client).



На этом настройка SSO закончена, и после применения политик, пользователь должен подключатся к ферме RDS по протоколу RDP без повторного ввода пароля.

Еще записи по теме: Windows Server 2012 R2

- FAQ по KMS активации продуктов Microsoft
- Настраиваем доменную аутентификацию на сетевом оборудовании
- Лицензирование Windows Server 2012 R2 и виртуализация
- Поддержка SMB 1.0 в Windows Server 2012 R2
- Защита Windows от уязвимости в SSL v3

Назад:
Уведомление о переходе на Windows 10

Вперед:
Перенос современных приложений Windows 10 на другой диск

Комментариев: 3

Оставить комментарий

Sasha Odarchuk | 24.10.2016

Указываем FQDN имя сервера RDCB и зону 2 (Trusted sites)
при RBCB HA указывать только DNS-имя для балансировки нагрузки (Round Robin) между серверами с ролью Connection Broker или перечислить еще и все RBCB-ы ?

Ответить

itpro | 11.11.2016

Указывается имя сервера, которое пользователь вводит в браузере, т.е. в вашем случае это fqdn имя RDCB

Ответить

Sasha Odarchuk | 21.11.2016

А если у меня для RDWA выделены отдельные сервера — мне тоже указывать fqdn имя RDCB ?? Просто при заходе на _https://fqdn имя RDCB/rdweb/pages я получаю ошибку что сайт не доступен

Ответить

Полные правила комментирования на сайте winitpro.ru.
Вопросы, не связанные с содержимым статьи или ее обсуждением удаляются.
Сказать **Спасибо!** можно на **этой** странице или (еще лучше) **поделиться с друзьями ссылкой** на понравившуюся статью в любимой социальной сети(специально для этого на сайте присуствуют кнопки популярных соц. сетей).

Ваш e-mail не будет опубликован. Обязательные поля помечены *

Имя * (обязательно)

E-mail * (обязательно)

Сайт

Я не робот(Обязательно отметьте)

b | i | del | link | b-quote | code | Close Tags

Отправить

Уведомлять меня по почте о новых комментариях

Поиск по сайту..

Подписка на новые статьи

Введите свой e-mail

Подписаться!

Серверные технологии Microsoft

- Active Directory
- Групповые политики

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- MS Exchange

» Все разделы

★ Клиентские технологии Microsoft

- Windows 10
- Windows 8
- Windows 7

» Все разделы

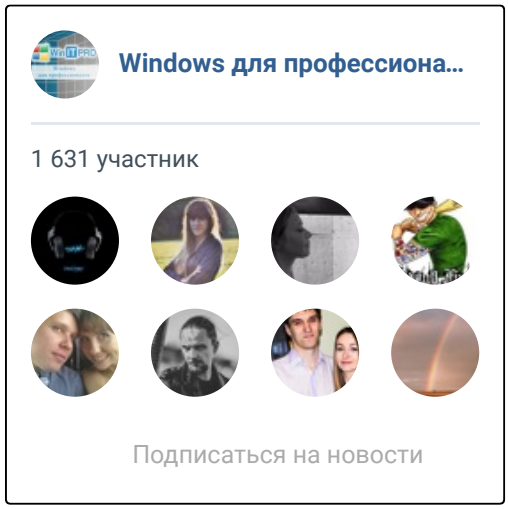
★ Разное

- VMWare
- Linux
- PowerShell
- Hewlett Packard

» Все разделы

Последние записи

Особенности лицензирования Exchange Server 2016 15/11/16



Последние комментарии

Кирилл: 17/12/16
Нехорошо закрывать контент банером адсенса...

Sasha Odarchuk: 15/12/16
Для того, чтобы этот командлет отрабатывал без ошибок на рабочей станции с Windo...

Sasha Odarchuk: 15/12/16
Пробую расширить диск. На самом сервере где хранятся UVHD делаю копию диска юзер...

Сергей: 15/12/16
По поводу команды "dism.exe /online /Cleanup-Image /StartComponentCleanup /Reset...

Sasha Odarchuk: 14/12/16
У меня RDS-ферма на Windows 2016 Std. Там стартовый экран работает ок. а вот с т...

Александр: 14/12/16
Были куплены лицензии 5 шт.- WS 2008R2 Std, с 3-х летней программой Open Value....

Alex Kornev: 14/12/16
"Те же яйца - вид сбоку". Без установки эпих заплаток (если их нет), даже с WSU...

ɸlex: 13/12/16
А если WSUS? Заметил недавно что с него тоже, rollup пока не ставил....

Интересные статьи

Лицензирование Windows Server 2012 R2 и виртуализация

FAQ по KMS активации продуктов Microsoft

FTP-сайт с изоляцией пользователей на Windows Server 2012 R2

Настройка VPN сервера на базе Windows Server 2012 R2

RDS Shadow – подключаемся к сессии пользователя в Windows 2012 R2

Установка KMS сервера на базе Windows Server 2012 R2

Простая система аудита удаления файлов и папок для Windows Server