Шаг 5. Настройка использования сертификатов для служб удаленных рабочих столов.

Posted on 06.09.2014

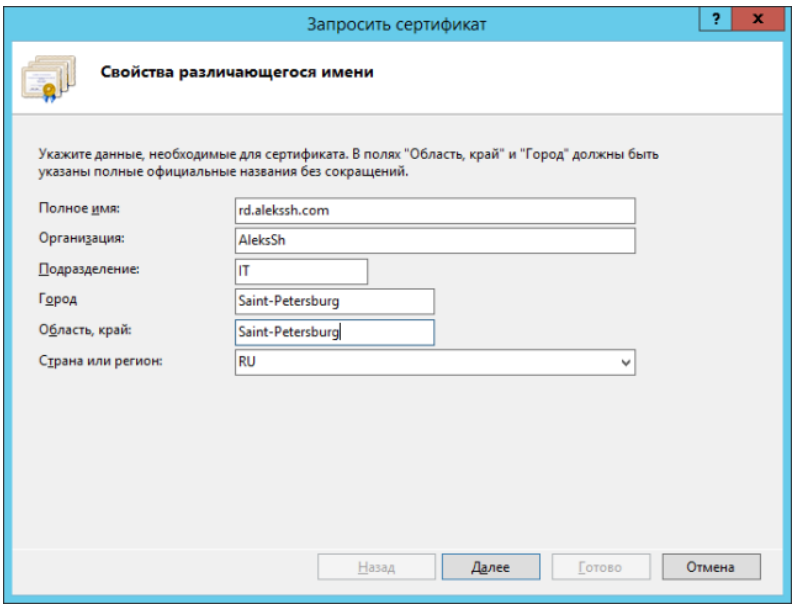
После установки ролей *Connection Broker, Web Access, Session Host и Gateway* крайне рекомендуется выполнить настройку сертификатов служб для обеспечения доверенного шифрованного соединения к удаленным приложениями. Вариантов использования сертификатов как обычно 3:

- использовать **самоподписанный**, который *придется* установить на все машины с которых будет происходить подключение.
- использовать **выданный доменным центром сертификации.** Для этого, естественно, потребуется развернутый доменный центр сертификации. Все доменные машины будут доверять выданному сертификату. Если же машина, с которой происходит подключение, находится не в домене, то на неё *придется* установить корневой сертификат центра сертификации.
- использовать **коммерческий (3rd party)**, который, исходя из названия, *придется* приобрести за деньги.

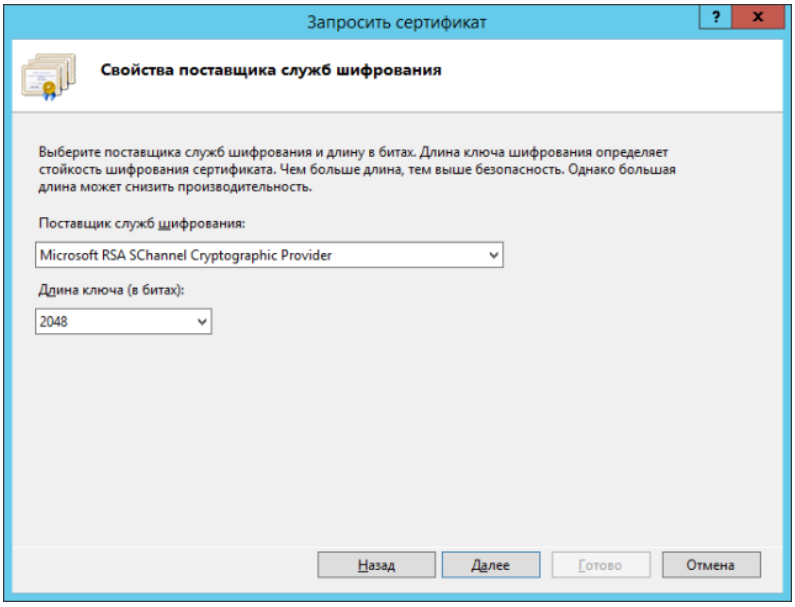
Плюсы и минусы использования любого из них очевидны. Я, все же, рекомендую, если есть возможность использовать коммерческий сертификат (в т.ч. wildcard), это позволит избежать проблем доверия сертификата, т.к. подавляющее большинство машин должно ему доверять, независимо от того находится машина в домене или нет.

Однако, в данном случае, я рассмотрю вариант использования сертификата, выданного **доменным центром сертификации**. Задача получить сертификат типа **.pfx**. Для этого сначала нужно подготовить запрос, самый простой способ, сделать его с имеющегося сервера с установленной ролью *IIS*. В данном случае все тот же **RDCB1**. В диспетчере служб IIS нужно перейти на «*Сертификаты сервера*» на начальной странице узла. Далее «*создать запрос сертификата*«.

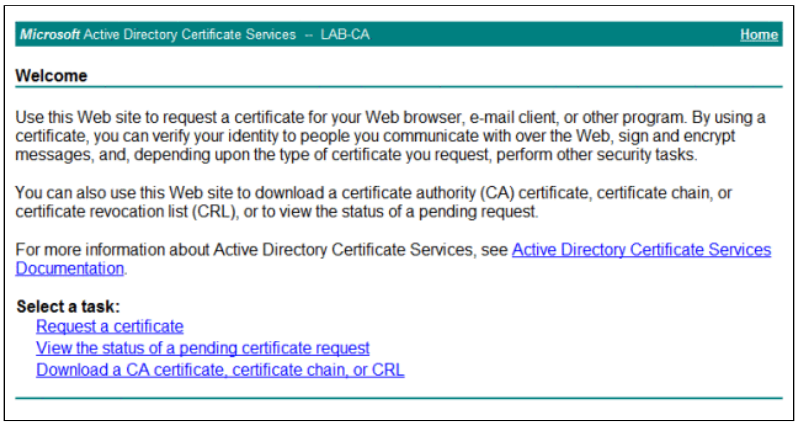
В запросе надо указать CN имя сертификата *RD.alekssh.com* и заполнить остальные поля.



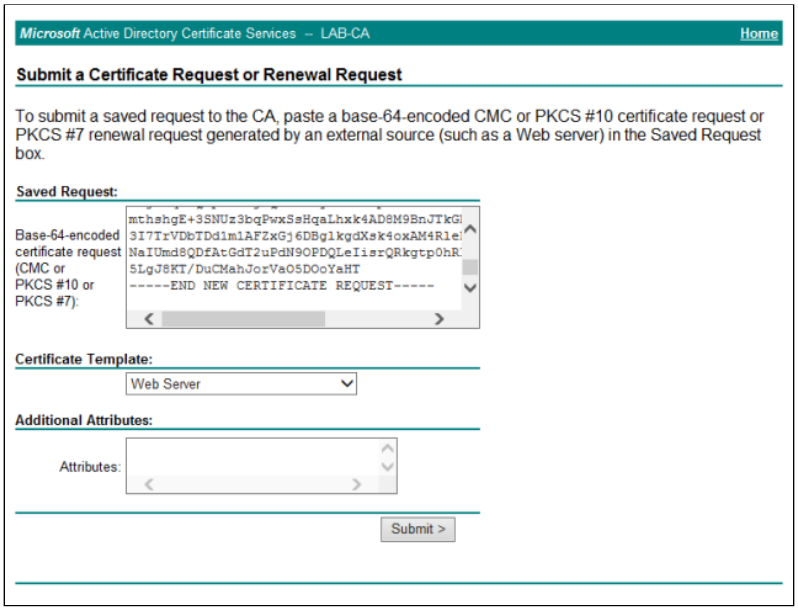
Выбрать длину ключа **2048**. И сохранить запрос в виде текстового файла.



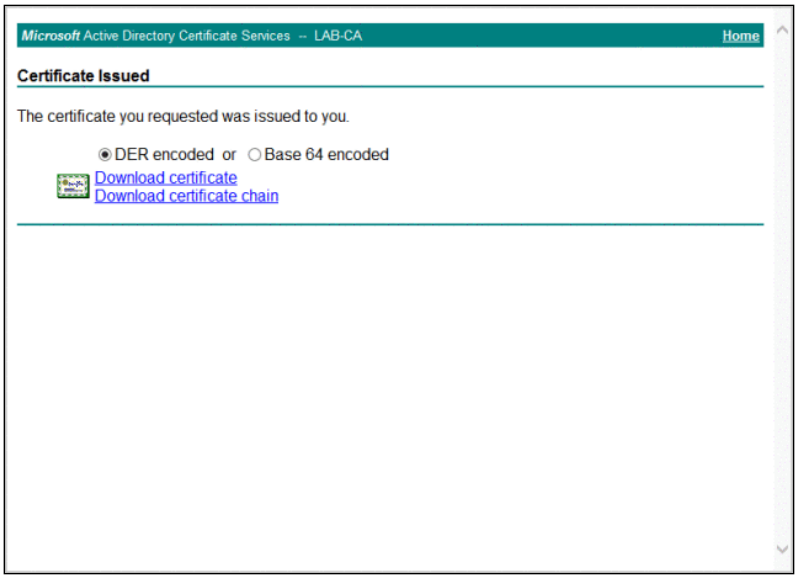
Далее перейти на веб страницу выдачи сертификатов, в данном случае *http://ca.lab.local/cersrv* и пройти по пути «*Request a certificate | Advanced certificate request | Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.*«



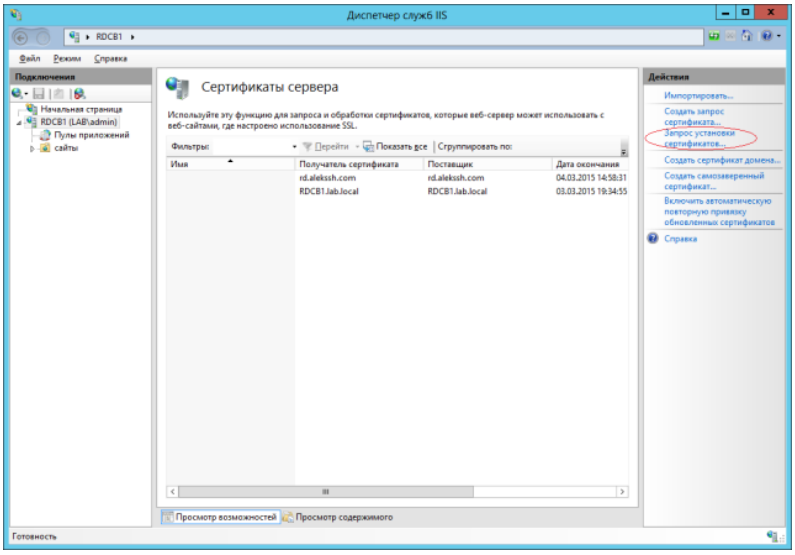
Далее вставить текст запроса из полученного текстового файла в поле *Saved Request* и выбрать «*Web Server*» в поле *Certificate Template*.



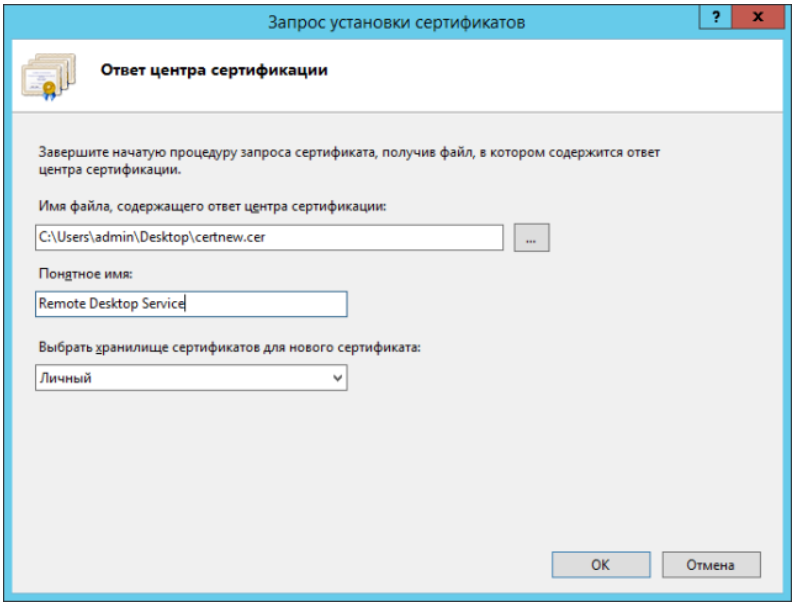
Далее скачать выданный сертификат .cer



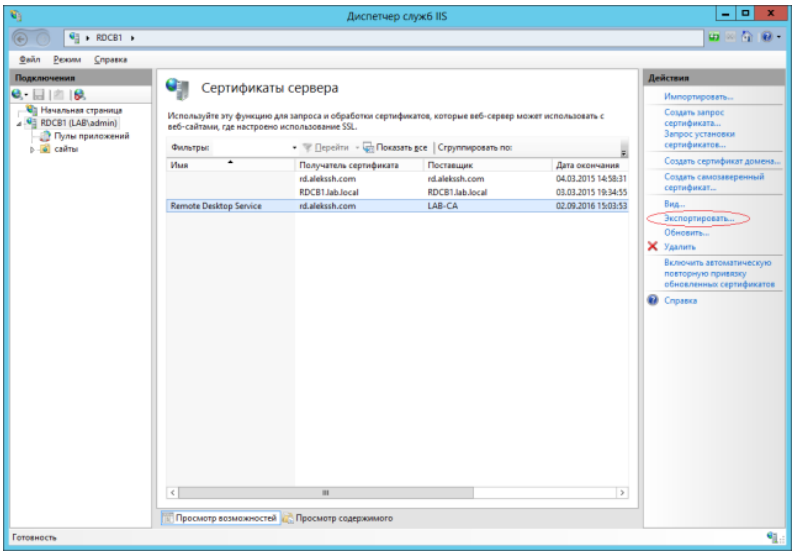
Теперь надо завершить запрос сертификата, для этого из Диспетчера служб IIS на том же сервере **RDCB1** надо запустить *«Запрос установки сертификатов»*.



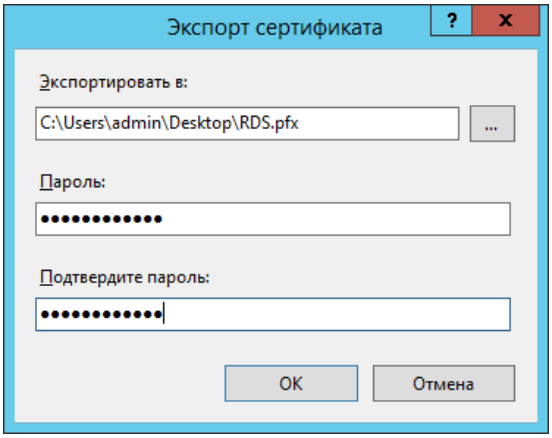
Выбрать полученный сертификат .cer и указать имя будущего сертификата .pfx. Затем завершить выпуск сертификата, нажав OK.



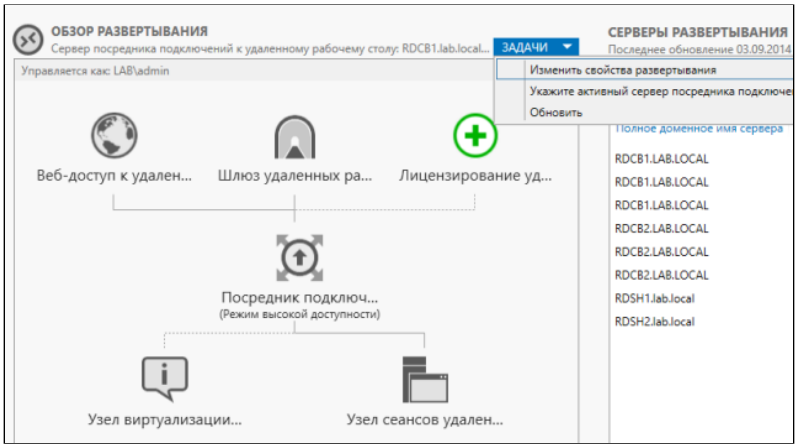
По итогам выпуска получится сертификат типа **.pfx**. Теперь его надо экспортировать для использования в ферме серверов.



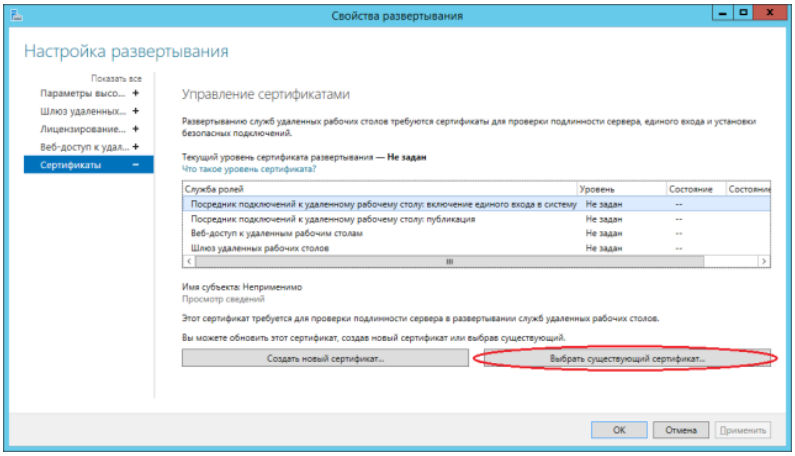
Указать папку для сохранения экспортируемого файла и пароль, с которым этот сертификат будет сохранен.



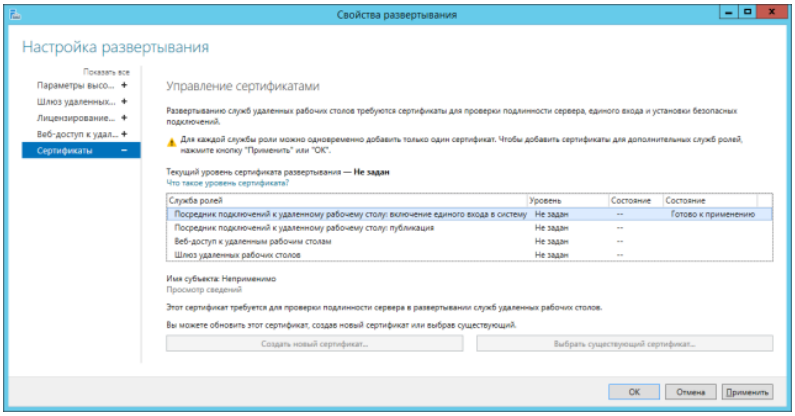
Для назначения сертификата службам удаленных рабочих столов нужно открыть Диспетчер серверов и выбрать *«Изменить свойства развертывания»*.



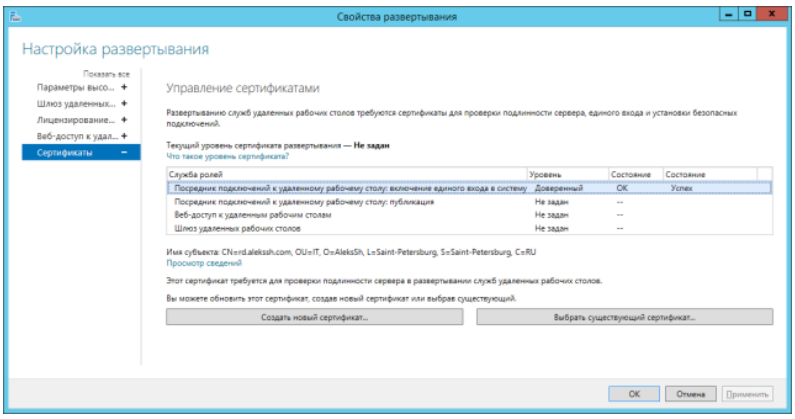
Далее назначить службам сертификат выбрав существующий, только что экспортированный сертификат **.pfx** с указанием пароля.



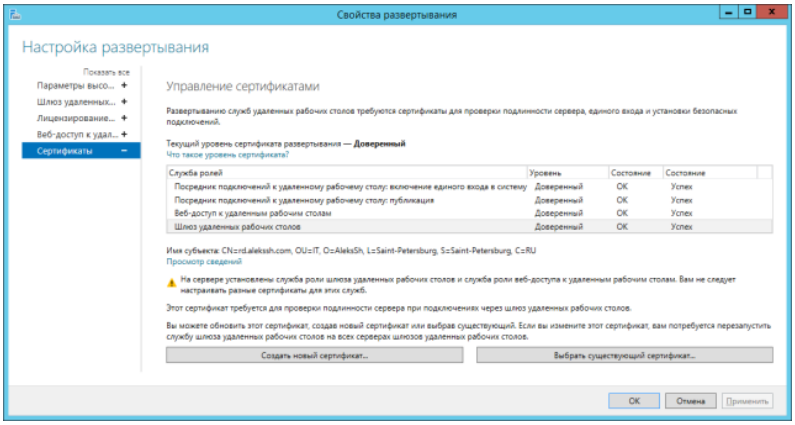
Далее применить конфигурацию.



Сертификат успешно назначен.



Повторить шаги для остальных служб.



Сертификаты служб настроены.

Далее настройка сервера лицензирования.

Информация, используемая в этой статье:

http://blogs.technet.com/b/askperf/archive/2014/01/24/certificate-requirements-for-windows-2008-r2-and-windows-2012-remote-desktop-services.aspx

http://technet.microsoft.com/ru-ru/library/cc732906(v=ws.10).aspx

Поделиться ссылкой:

★ Нравится

Будьте первым, кому это понравилось.

Связанные

Шаг 3. Настройка высокой доступности Веб доступа (Web Access High Availability)
В "RDS 2012 R2"

Шаг 4. Настройка высокой доступности Шлюза удаленных рабочих столов (RD Gateway High Availability).
В "RDS 2012 R2"

Шаг 1. Первоначальная установка основных служб удаленный рабочих столов.
В "RDS 2012 R2"

Об авторе Alexander Shestakov
MCITP, MCSE. Компания "Динамика"
Посмотреть все записи автора Alexander Shestakov →

Запись опубликована в рубрике RDS 2012 R2 с метками Пример использования сертификатов удаленнных рабочих столов, RDS 2012 R2, RDS 2012 R2 Certificates, RDS 2012 R2 сертификаты. Добавьте в закладки постоянную ссылку.

14 комментариев на «*Шаг 5. Настройка использования сертификатов для служб удаленных рабочих столов.*»

alexey:
09.06.2016 в 12:23

как быть в случае с несколькими узлами сеансов удаленных рабочих столов? посредник, веб-доступ — на одном компе

★ Нравится
Ответить

Alexander Shestakov:
09.06.2016 в 12:30

Расскажите подробнее в чем вопрос?

★ Нравится
Ответить

alexey:
09.06.2016 в 12:36

есть server windows 2012 r2. на нем установлены роли посредник, веб-доступ, лицензирования, узел сеансов. создаю по вашей статье сертификат pfx. в свойствах развертывания указываю его у всех ролей (кроме шлюз). в iis соотвественно тоже.

есть server1 windows 2012 (на hyper-v) на нем установлена лишь роль узла сеансов.

создаю 2 коллекции в каждой по 1 узлу сеансов. в каждой коллекции публикую 1 программу.

в rdweb вижу 2 иконки, скачиваются 2 rdp файла.
прога на server — открывается нормально.

на server1 — выдается сообщение, что программа отсутствует в списке разрешенных remoteapp программ. притом подключение производится к server.
rdp-файл генерируется неправильно.

я подумал, что это связано с сертификатами для RDS

★ Нравится
Ответить

alexey:
09.06.2016 в 12:38

забыл уточнить. что если переустановить роль rds на server уже без сертификатов. то подключение производится нормально за исключением того, что выдается сообщение о недоверенном подключении rdp

★ Нравится

Alexander Shestakov:
09.06.2016 в 12:45

не ваш ли случай? https://social.technet.microsoft.com/Forums/ru-RU/dd4be1d1-354e-4d0d-9183-1b9a031fbc5f/remoteapp-?forum=WS8ru

★ Нравится

alexey:
09.06.2016 в 13:26

нет. не мой.
у меня вопрос в чем: если есть 2 узла сеансов, один посредник и один сервер с веб-доступом. то сертификаты в свойствах развертывания я задаю одинаковый для посредник включение единого входа в систему, посредник публикация и веб-доступ?

★ Нравится
Ответить

Alexander Shestakov:
09.06.2016 в 15:37

У вас один сервер к которому обращаются пользователи, для него и нужен сертификат. Для второго узла сеансов отдельный сертификат не нужен, да и назначить отдельно не получится. Посредник будет перенаправлять подключения на нужный узел сеансов. Действительно ли есть необходимость в двух коллекциях?

★ Нравится
Ответить

Ammyy Admin:
25.07.2016 в 08:47

В ASA можно воспользоваться несколькими командами группы show в командной строке для проверки статуса сертификата.

★ Нравится
Ответить

odarchuk:
23.10.2016 в 23:35

Какие FQDN нужно указать при заказе ком. сертифката ?
Хотим использовать один сертификат для всех и вся🙂
вайлкард — не предлагать🙂
я пока нашел 3 имени: RD GW + RD CB + RD WA — ничего не забыл ?

★ Нравится
Ответить

Alexander Shestakov:
24.10.2016 в 10:58

Я так понимаю вам нужен коммерческий сертификат для внешнего доступа. Для терминальной фермы, как для публикации веб доступа, RemoteApp так и RD Gateway достаточно одного имени, того, к которому будут осуществляться подключение. В моем случае внешнее имя rd.alekssh.com.

★ Нравится
Ответить

Alexander Shestakov:
24.10.2016 в 10:59

Кстати, wildcard прекрасно работает🙂

★ Нравится
Ответить

Евгений:
23.11.2016 в 10:17

Отличные статьи! собираю на виртуалках подобную схему. Прошел шаги 0-4. На пятом понял, что нужен «доменный центр сертификации» Разрозненная информацию есть на многих сайтах. С удовольсвием почитал-бы ваше дополнение к этому циклу статей. Размышления о том с какими ролями совмещать роль центра сертификации, как обеспечить высокодоступность.

★ Нравится
Ответить

Alexander Shestakov:
23.11.2016 в 11:40

Спасибо. В данном случае, центр сертификации развернут на контроллере домена, настроны роли CA и CA Web Enrollment. Если же есть необходимость настроить центр сертификации, что называется, «по-взрослому», с оффлайновым корневым центром и прочим, то очень рекомендую цикл статей Вадима Поданса https://www.sysadmins.lv/blog-ru/ustanavlivaem-certification-authority-podvedenie-itogov.aspx если рекомендовать то лучшее🙂

★ Нравится
Ответить

Евгений:
23.11.2016 в 12:21

Спасибо за оперативный ответ! сейчас как раз читал https://www.sysadmins.lv/blog-ru/obsuzhdenie-shem-ierarhii-certification-authority.aspx

★ Нравится

Ответить
