Microsoft Azure Backup + КриптоПро + Аладдин РД

Руководство по настройке

Версия документа:	1.0
Редакция от:	15 мая 2014 г.
Листов:	29

Аннотация

Настоящий документ содержит сведения по настройке резервного копирования информации в облако Microsoft Azure Backup зашифрованной при помощи КриптоПро EFS и доступа к этой информации по USB-токенам и смарт-картам компании «Аладдин Р.Д.».

Оглавление

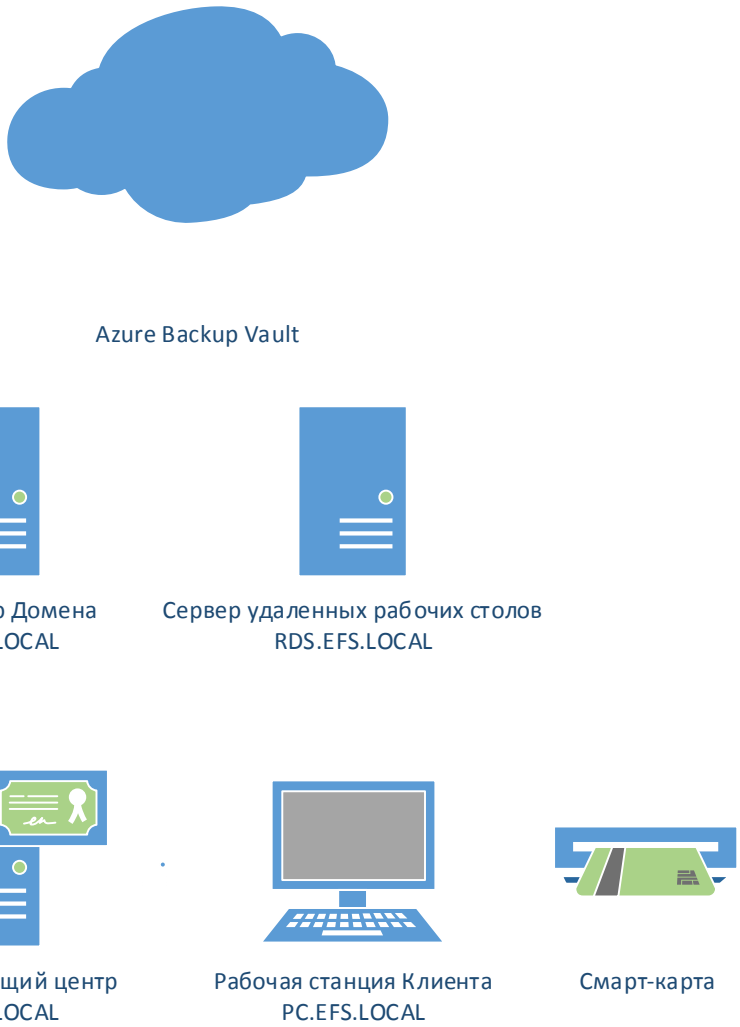
Описание демо инфраструктуры

В организации EFS находятся три сервера на основе ОС Windows Server 2012 R2

- DC.EFS.LOCAL - Контроллер Домена Active Directory
- RDS.EFS.LOCAL – Сервер удаленных рабочих столов
- CA.EFS.LOCAL – Будущий удостоверяющий центр и центр выдачи сертификатов

Сотрудники организации подключаются к RDS.EFS.LOCAL для доступа к приложениям и хранят на нем свои рабочие документы.

Необходимо обеспечить защищенность данных, путем их шифрования и осуществления резервного копирования в георасределенное облачное хранилище Microsoft Azure. Доступ к данным осуществляется по закрытому ключу, который безопасно хранится на USB-токене или смарт-карте.

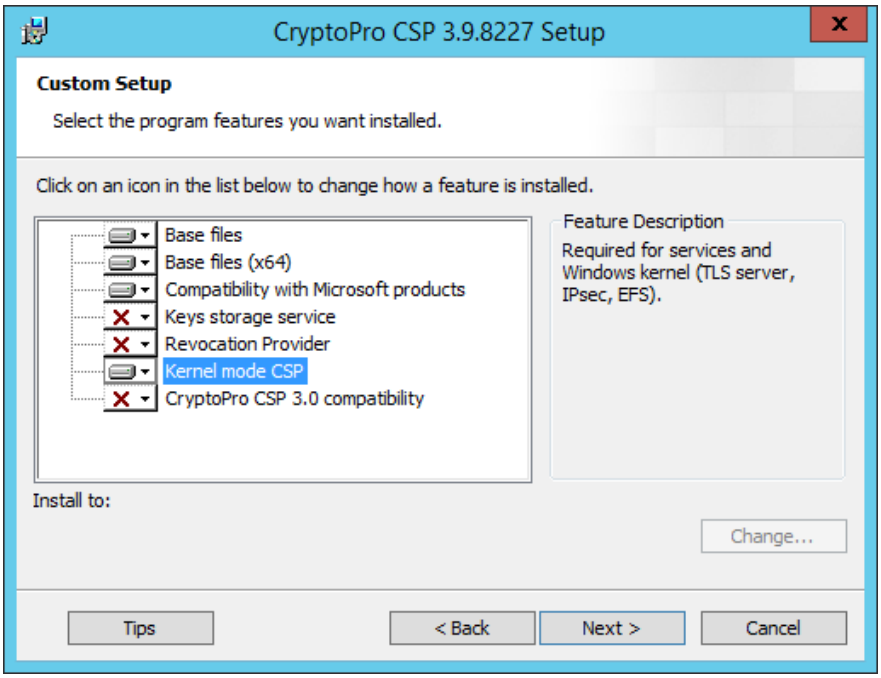


Установка необходимого ПО

Установка КриптоПро CSP

ПО КриптоПРО CSP в настоящем примере необходимо установить на:
контроллер домена DC.EFS.LOCAL;
сервер рабочих столов RDS.EFS.LOCAL;
сервер центра сертификации CA.EFS.LOCAL;
клиентские машины PC.EFS.LOCAL.

Во время установки выберите тип — **Выборочная** и отметьте для установки компонент **Kernel mode CSP.**



Установка SafeNet Authentication Client

На все ПК и серверы, где планируется использование смарт-карт, установите **ПО SafeNet Authentication Client.**

Установку производите с параметрами по умолчанию.

Установка КриптоПро EFS

На ПК пользователей и сервер удаленных рабочих столов установите ПО **КриптоПро EFS.**

Установку производите с параметрами по умолчанию.

Установку следует производить, только после установки **КриптоПро CSP.**

Подготовка учетных записей и групп

В настоящем примере используются 3 учетные записи и 2 группы. Для демонстрации понадобятся следующие учетные записи:

Учетные записи:

1. **DCAdmin** — учетная запись администратора предприятия.
2. **efsRA** — учетная запись агента восстановления EFS.
3. **K.Sobchak** — учетная запись рядового пользователя.

Группы:

4. **EFSUsers** — пользователи, которым будут использовать EFS шифрование
5. **EFS Computers** — компьютеры на которых будет включено EFS шифрование

В группу **EFSComputers** необходимо включить компьютеры, на которых будет задействовано EFS шифрование с использованием ГОСТ-алгоритма. В настоящем примере это будет **RDS.EFS.LOCAL.**

Настройка Центра Сертификации

Установка роли центра сертификации

В настоящем примере используется упрощённая установка центра сертификации (далее ЦС) с использованием только корневого ЦС.

На сервере **CA.EFS.LOCAL** добавьте роль центра сертификации: **Диспетчер сервера -> Управление -> Добавить роли и компоненты.**

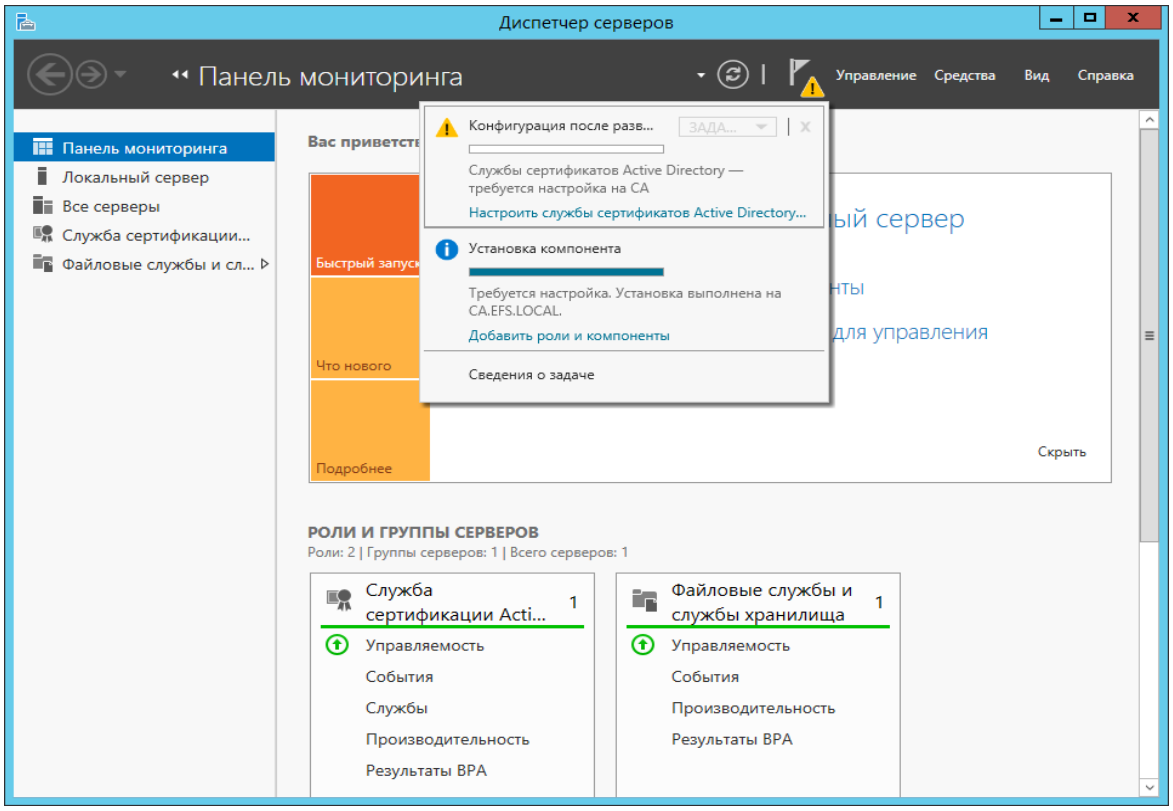
С помощью мастера добавления ролей и компонентов выберите для установки роль **Службы сертификатов Active Directory.**

При выборе службы ролей необходимо выбрать **Центр сертификации.**

Настройка службы центра сертификации

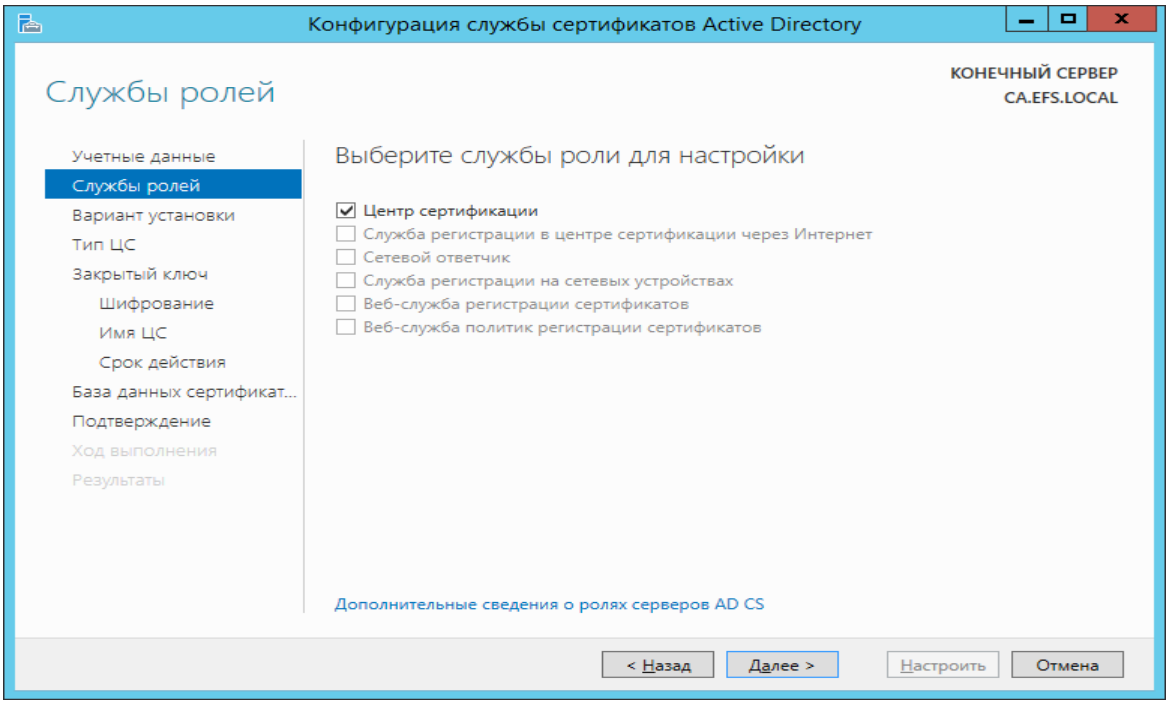
После завершения установки службы сертификатов необходимо ее настроить.

1. Из **Диспетчера серверов** вызовите диалог настройки службы.

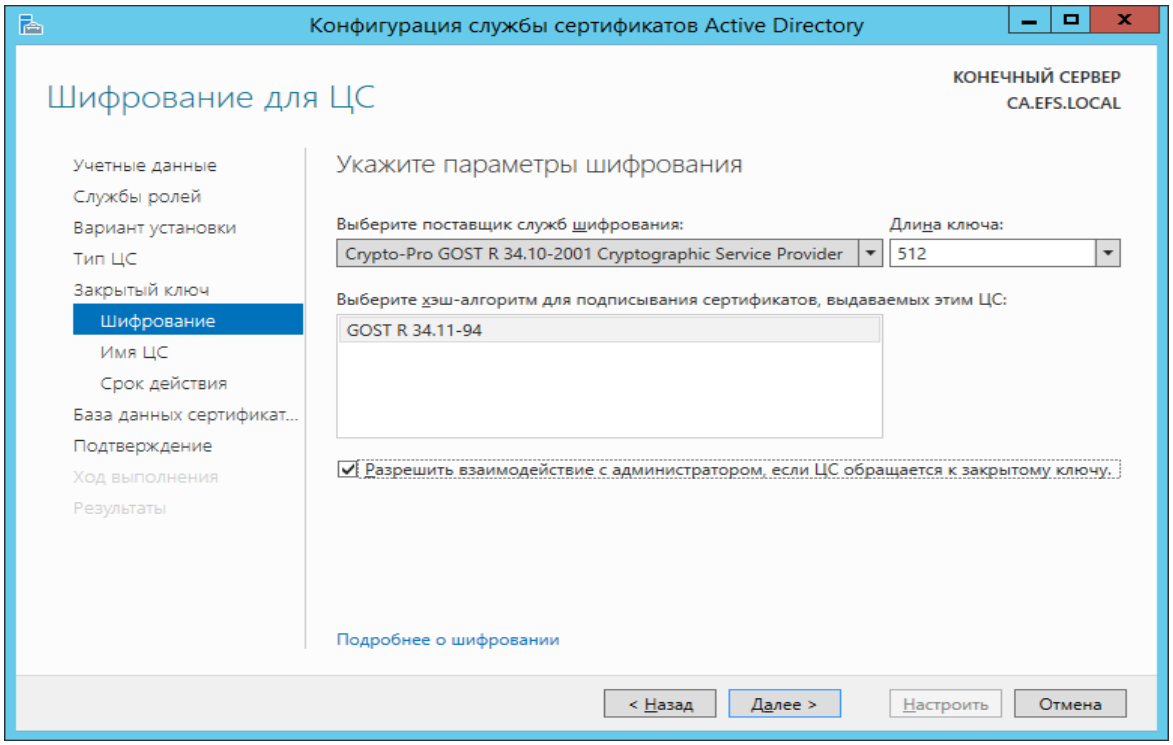


2. Введите учетные данные пользователя, входящего в группу **Администраторы предприятия.**

3. В качестве службы для настройки выберите **Центр сертификации.**



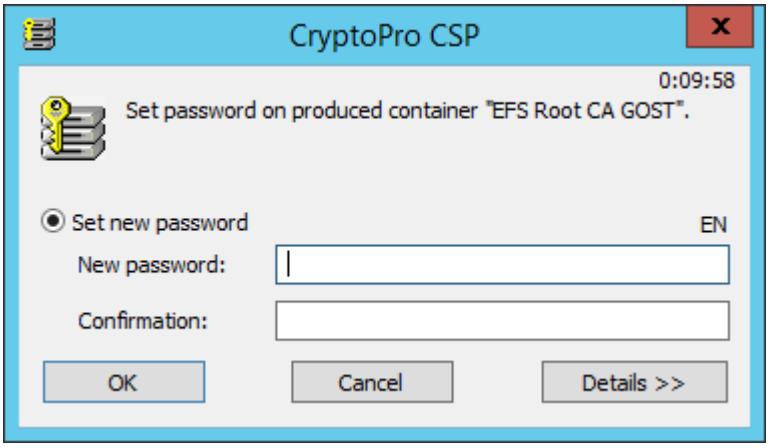
4. Укажите вариант установки центра сертификации — **ЦС Предприятия.**
5. Укажите тип центра сертификации — **Корневой ЦС.**
6. Укажите тип закрытого ключа — **Создать новый закрытый ключ.**
7. Задайте параметры шифрования согласно рисунку.



8. Имя ЦС можно оставить в значении по умолчанию.
9. Срок действия установите — 5 лет.

10. Расположение баз данных можно оставить в значении по умолчанию.
11. Нажмите кнопку **Настроить.** Далее отобразится запрос на выбор расположения контейнера закрытого ключа (далее ЗК).
12. **Выберите Реестр (Registry).**

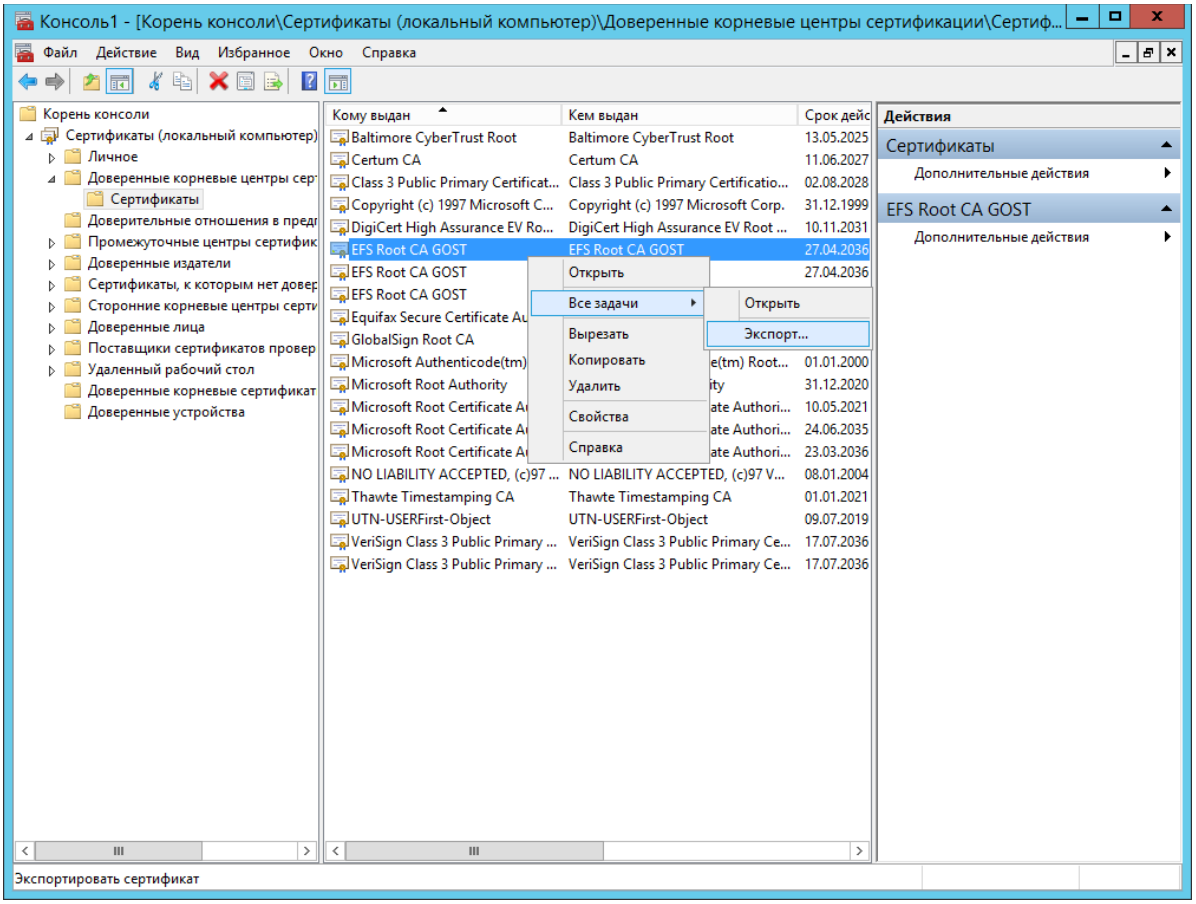
13. После ввода произвольной последовательности для генерации ключа отобразится диалог ввода ПИН-кода. Задайте ПИН-код для контейнера ЗК.



14. Первоначальная настройка ЦС на этом закончена.

Экспорт сертификата ЦС

Выполните экспорт сертификата ЦС в файл, доступный для контроллера домена. Для этого воспользуйтесь оснасткой **Сертификаты (локальный компьютер).**

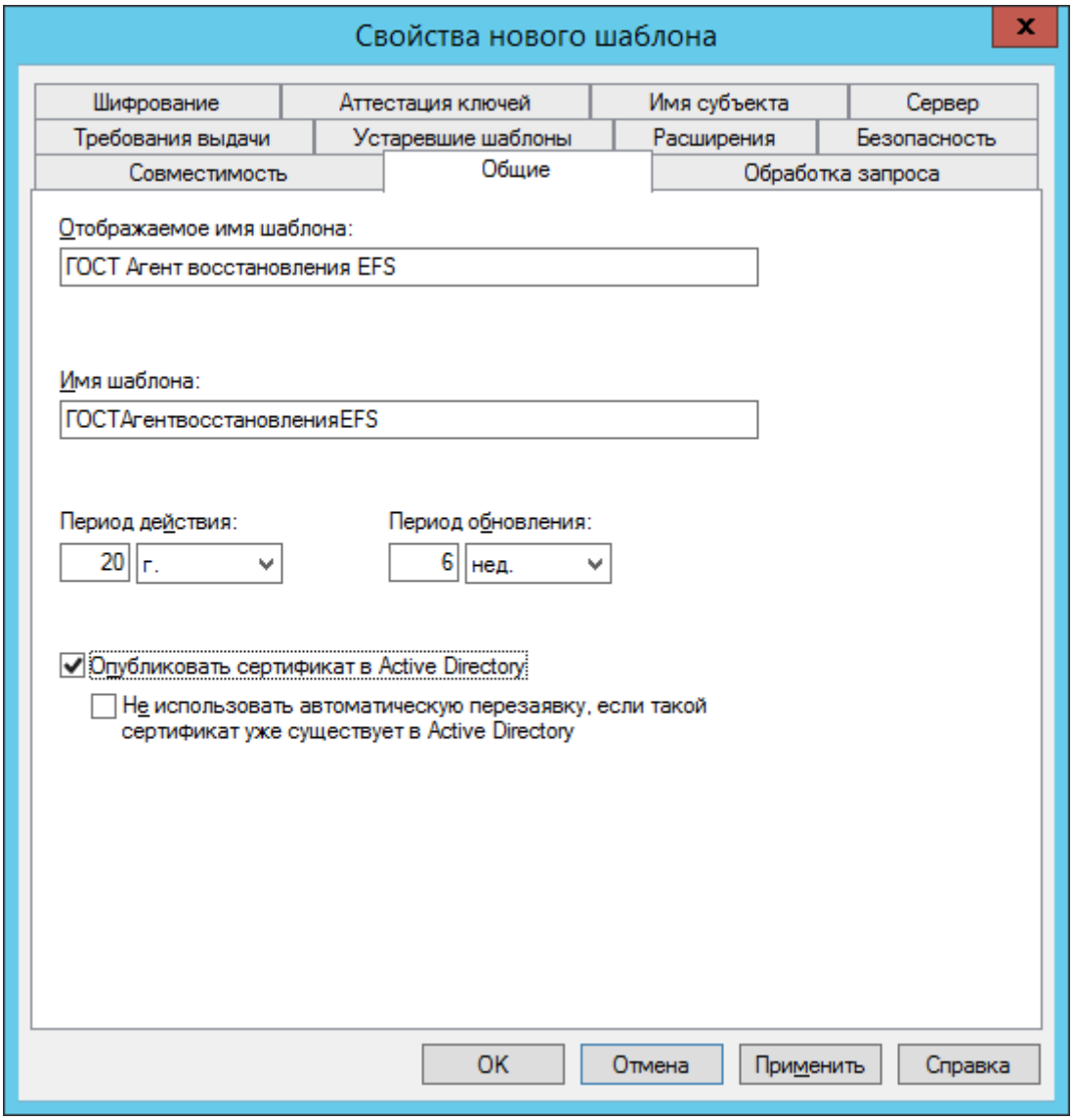


Задайте произвольное имя сертификата, например **efs_root_ca.cer.**

Настройка шаблонов сертификатов

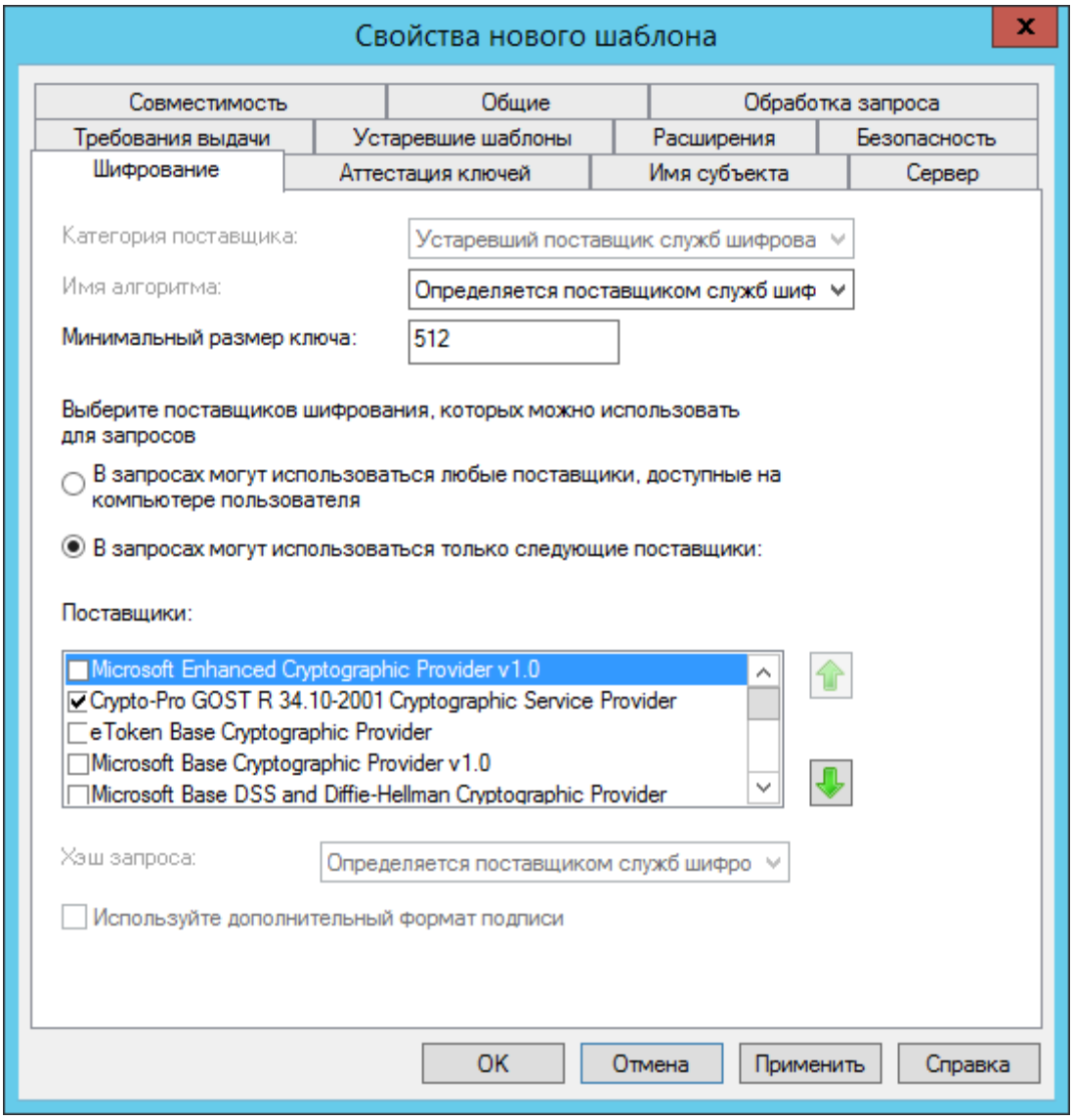
1. Откройте оснастку **Центр сертификации** из **Диспетчера серверов -> Средства.**
2. Далее **Шаблоны сертификатов -> Действие -> Управление**

3. Скопируйте шаблон **Агент восстановления EFS**, в появившемся окне переименуйте поле **Отображаемое имя шаблона.**

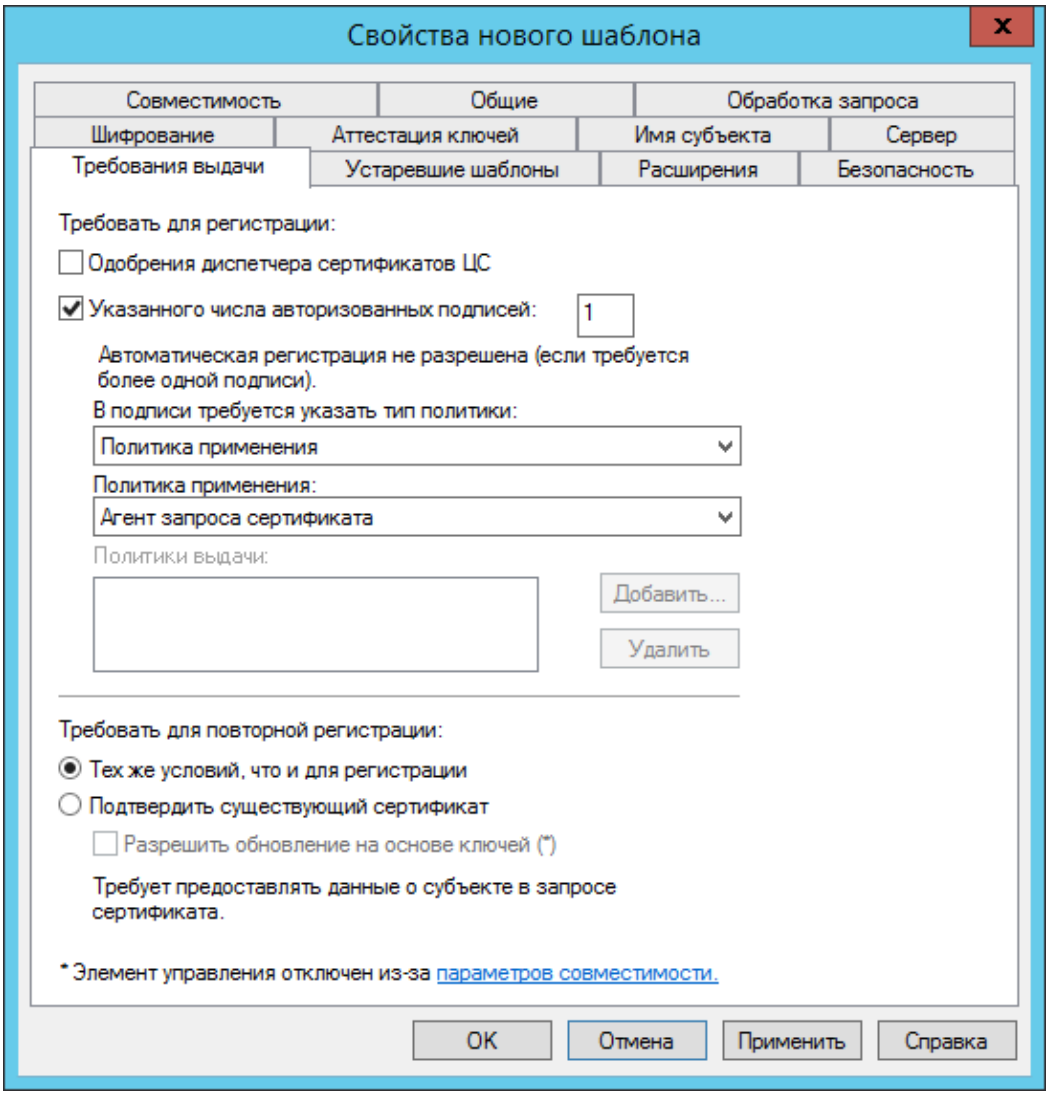


4. Установите галочку Опубликовать сертификат в Active Directory.
5. На вкладке Обработка запроса снимите галочку Разрешить экспортировать закрытый ключ

6. На вкладке шифрование выставьте параметры, как показано на рисунке.



7. На вкладке **Требования выдачи** выставьте следующие настройки.



8. На вкладке **Безопасность** добавьте пользователя, который будет выдавать ключи другим пользователям.
9. Разрешите этому пользователю **Чтение, Запись** и **Заявка**.
10. Аналогично выполняется конфигурация шаблонов **Базовое шифрование EFS**, **Вход со смарт-картой** и **Агент регистрации.**

Публикация шаблонов

1. В списке шаблонов сертификатов удалите шаблоны **Агент восстановления EFS** и **Базовое шифрование EFS**.
2. Вместо них добавьте только что созданные шаблоны: **Шаблоны сертификатов -> Действие -> Создать -> Выдаваемый шаблон сертификата.**

Инициализация и выпуск ключей

Процедура инициализации ключей

Необходимо инициализировать три ключа для пользователей: **DCAdmin**, **efsRA**, **K.Sobchak**.

Выпуск сертификата Агента регистрации

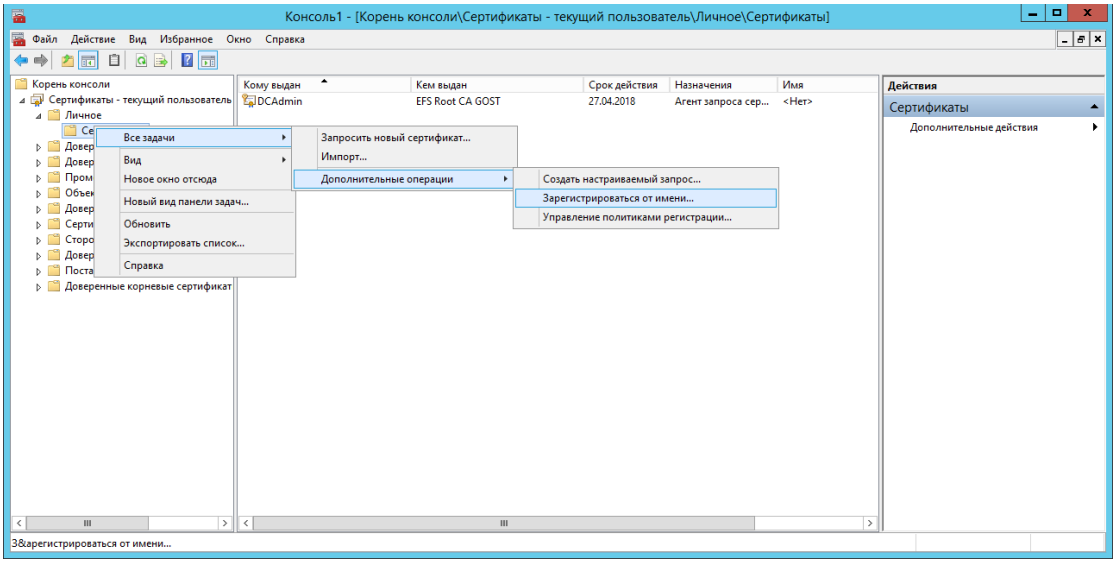
В качестве агента регистрации, в настоящем примере, используется учетная запись **DCADmin.**

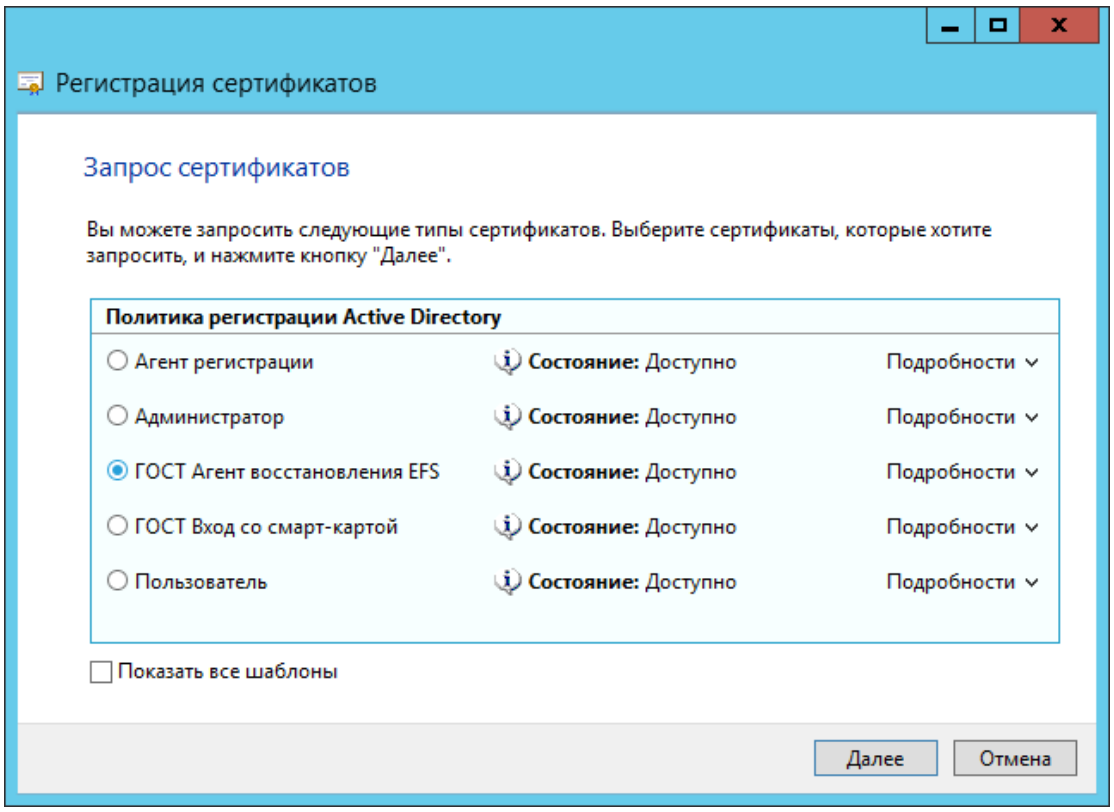
Войдите пользователем **DCAdmin** на **CA.EFS.LOCAL** и из оснастки **Сертификаты –> текущий пользователь** запросите сертификат **ГОСТ Агент регистрации.**
В качестве контейнера используйте **смарт-карту** (для **DCADmin**).

После выпуска сертификата агента регистрации, появляется возможность выпускать сертификаты для других пользователей от имени **DCADmin.**

Выпуск сертификата Агента восстановления EFS

Из-под пользователя **DCAdmin** при помощи оснастки **Сертификаты – >текущий пользователь** выполните запрос сертификата **ГОСТ Агент восстановления EFS** для пользователя **efsRA**.





Выпуск сертификата производите на **смарт-карту** предназначенную для **efsRA**.

Этот сертификат экспортируйте в файл

Аналогично произвести выпуск сертификата **ГОСТ Вход со смарт-картой.**

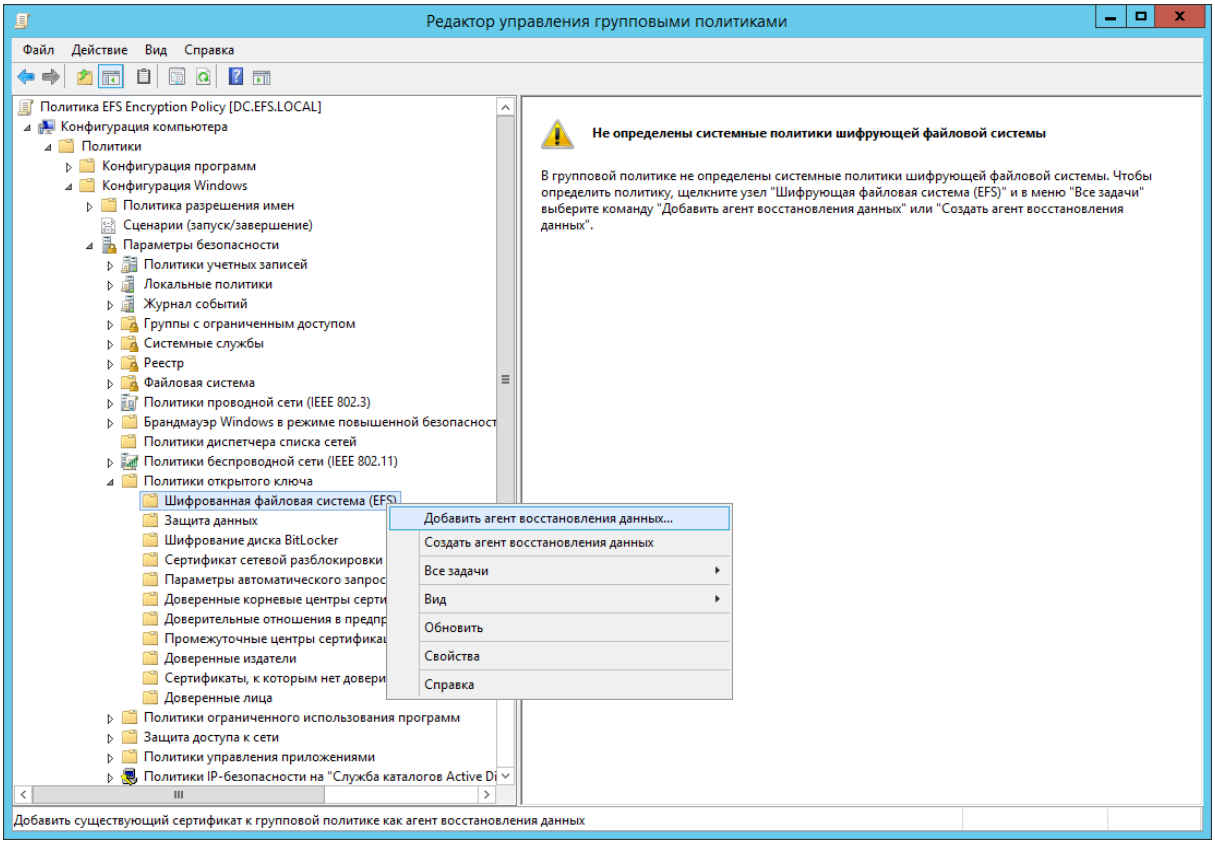
Выпуск сертификата Пользователя

Выполняется аналогично предыдущему, только необходимо использовать шаблоны **ГОСТ Базовое шифрование** и **ГОСТ Вход со смарт-картой.**

Настройка групповых политик

Настройка Агента восстановления

1. Создайте групповую политику **EFS Encryption Policy** применяемую к группе **EFSComputers.**
2. В политике компьютера **Конфигурация Windows -> Параметры безопасности -> Политики работы с открытыми ключами -> Шифрованная файловая система EFS->Добавить агента восстановления данных.**



3. Добавить сертификат **efsra.cer.**
4. В свойствах **Шифрованная файловая система (EFS)** на вкладке **Общие** отметьте **Разрешить Шифрование файлов с помощью шифрующей файловой системы (EFS).**
   А на вкладке **Сертификаты** снять галочку **Разрешить EFS создавать самозаверяющиеся сертификаты, если центр сертификации недоступен.**

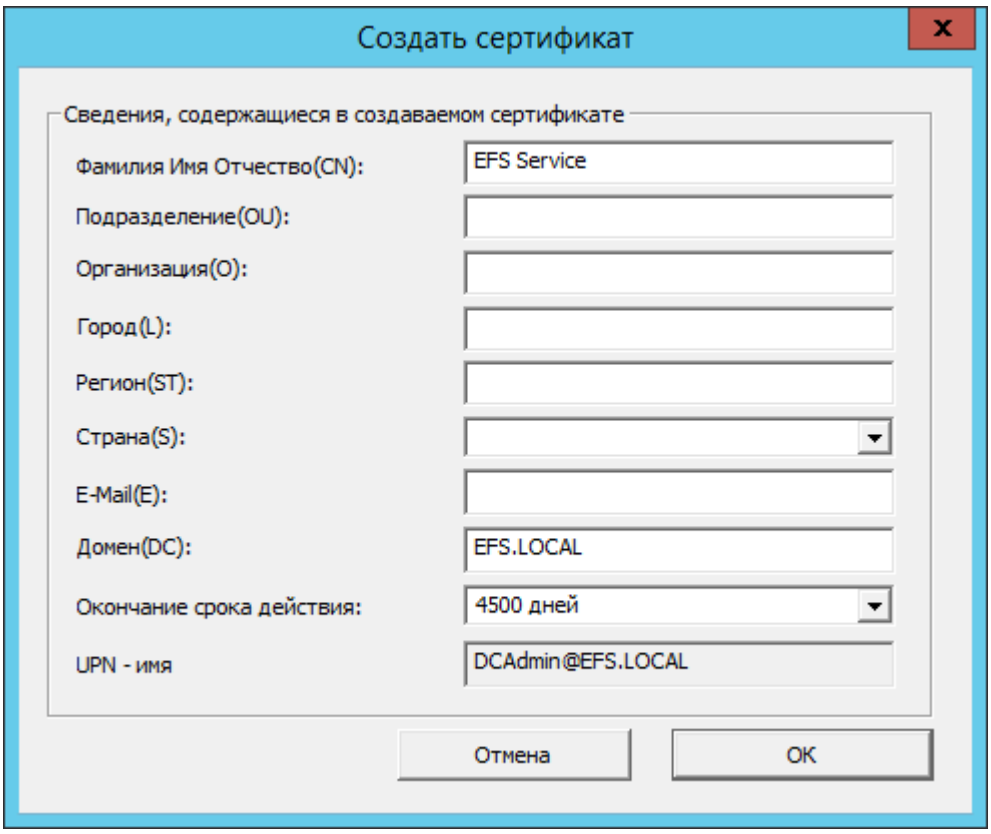
Добавление сертификата ЦС в хранилище доверенных сертификатов

Необходимо добавить сертификат ЦС в список доверенных центров сертификации.

Для этого создайте политику **Trusted Certificates** и в секции **Конфигурация компьютера -> Политики-> Конфигурация Windows -> Параметры безопасности ->Политика открытого ключа-> Доверенные корневые центры сертификации -> Импорт.** Выберите сертификат **efr_root_ca.cer.**

Настройка сервера RDS

Выпустите служебный, самоподписанный сертификат при помощи утилиты **Консоли управления КриптоПРО EFS.**
Мои сертификаты -> Все задачи -> Создать самоподписанный сертификат.



Далее выполните экспорт сертификата из оснастки **Сертификаты - текущий пользователь** в двух форматах: с экспортом закрытого ключа (.pfx) и без экспорта закрытого ключа (.cer).

Сертификат с закрытым ключом .pfx импортируйте в **Личное** хранилище компьютера, а сертификат без закрытого ключа .cer в хранилище **Доверенные лица** компьютера.

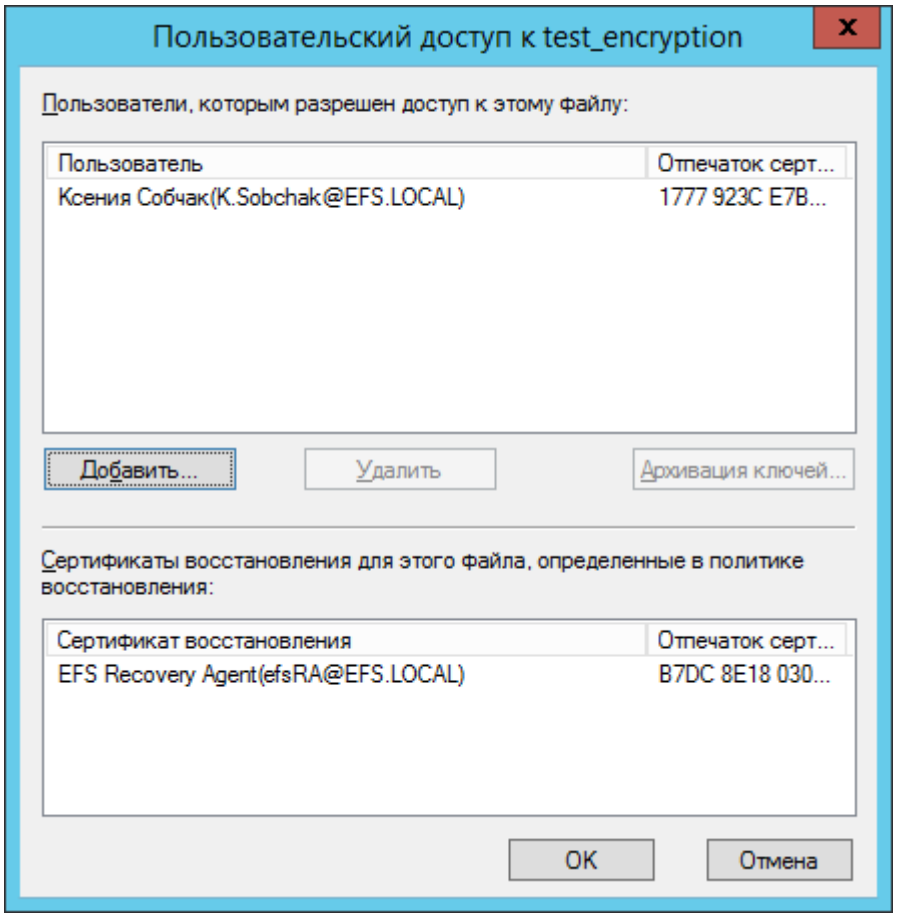
ПИН-код при импорте оставьте пустым.

Шифрование файлов

Теперь можно проверить шифрование файлов на **RDS.EFS.LOCAL.** Для этого подключитесь, при помощи смарт-карты к серверу RDS.

В каталоге Документы, создайте файл и зашифруйте его, выставив в свойствах файла **Другие -> Шифровать содержимое для защиты данных.**

Нажмите кнопку **Подробно**, если все прошло без ошибок, отобразиться следующее окно.

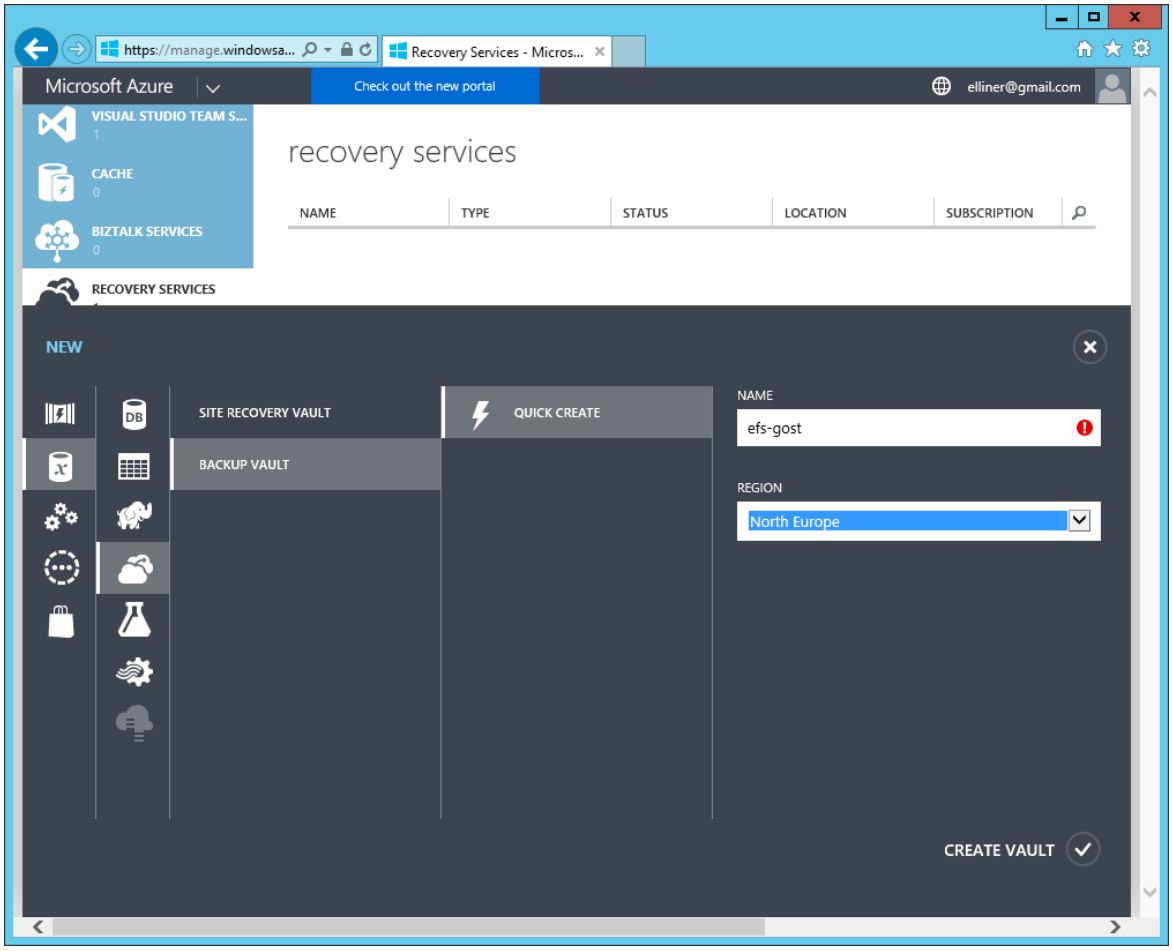


Настройка резервного копирования в облако Azure

Регистрация хранилища Azure

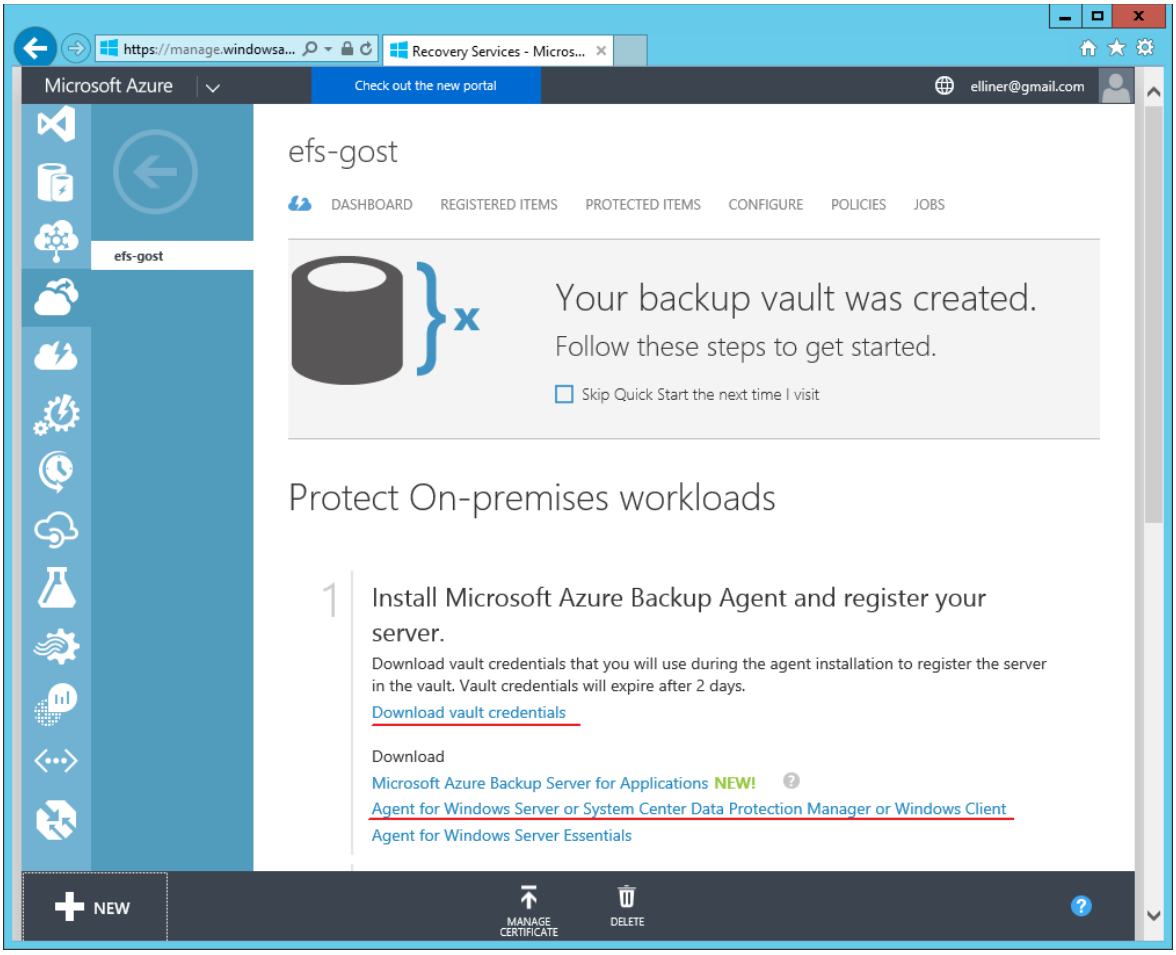
Для запуска резервного копирования, необходимо зарегистрировать новое хранилище в Azure.

Для этого перейдите по ссылке http://manage.windowszure.com. Далее войдите под учетной записью Microsoft, в пункте меню **Recovery Services.** Перейдите к пункту **NEW ->Recovery Services ->Backup Vault ->Quick Create**



Задайте имя хранилища, например **efs-gost.** И выберите регион хранения данных, например **North Europe.**

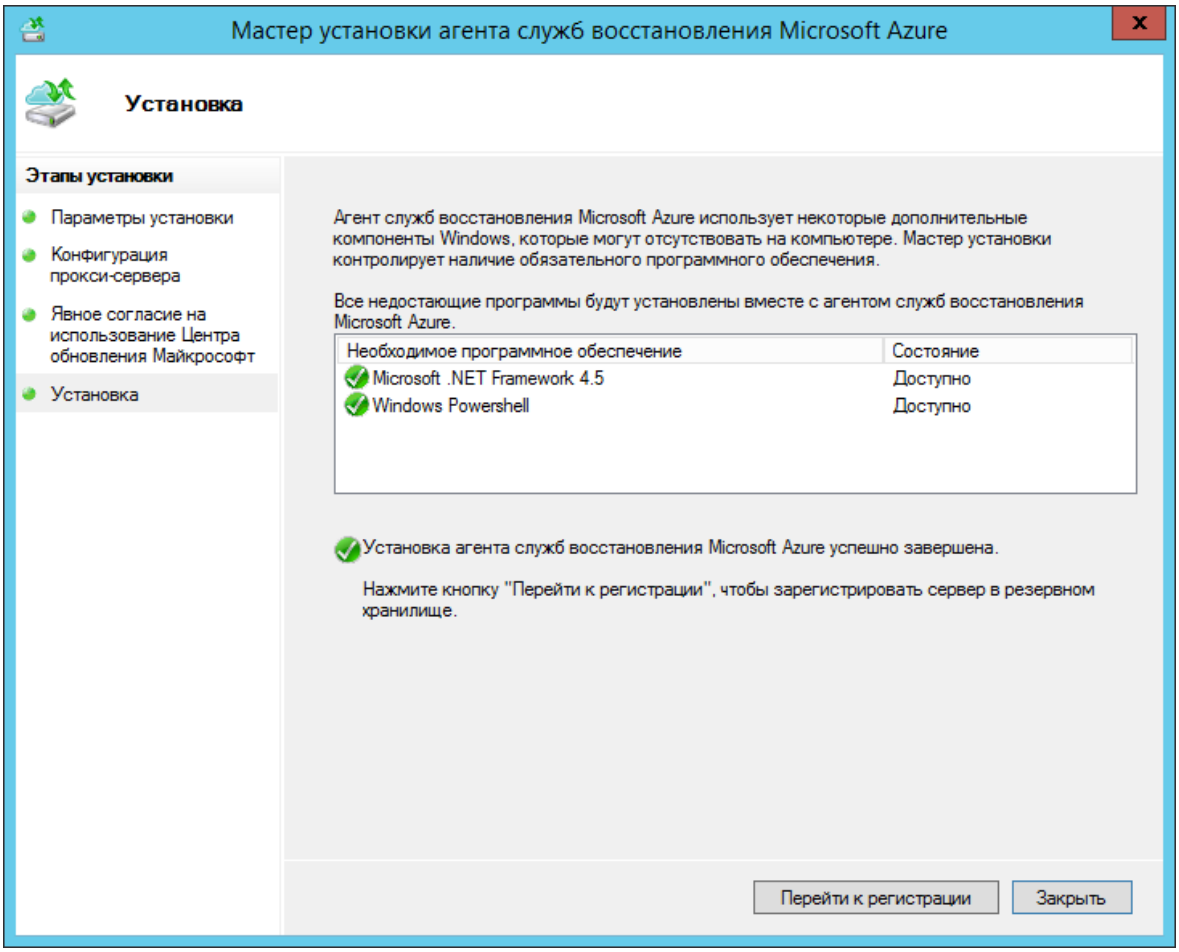
После создания хранилища скачайте файл учетных данных и клиент **Azure Backup** по предоставленным ссылкам.



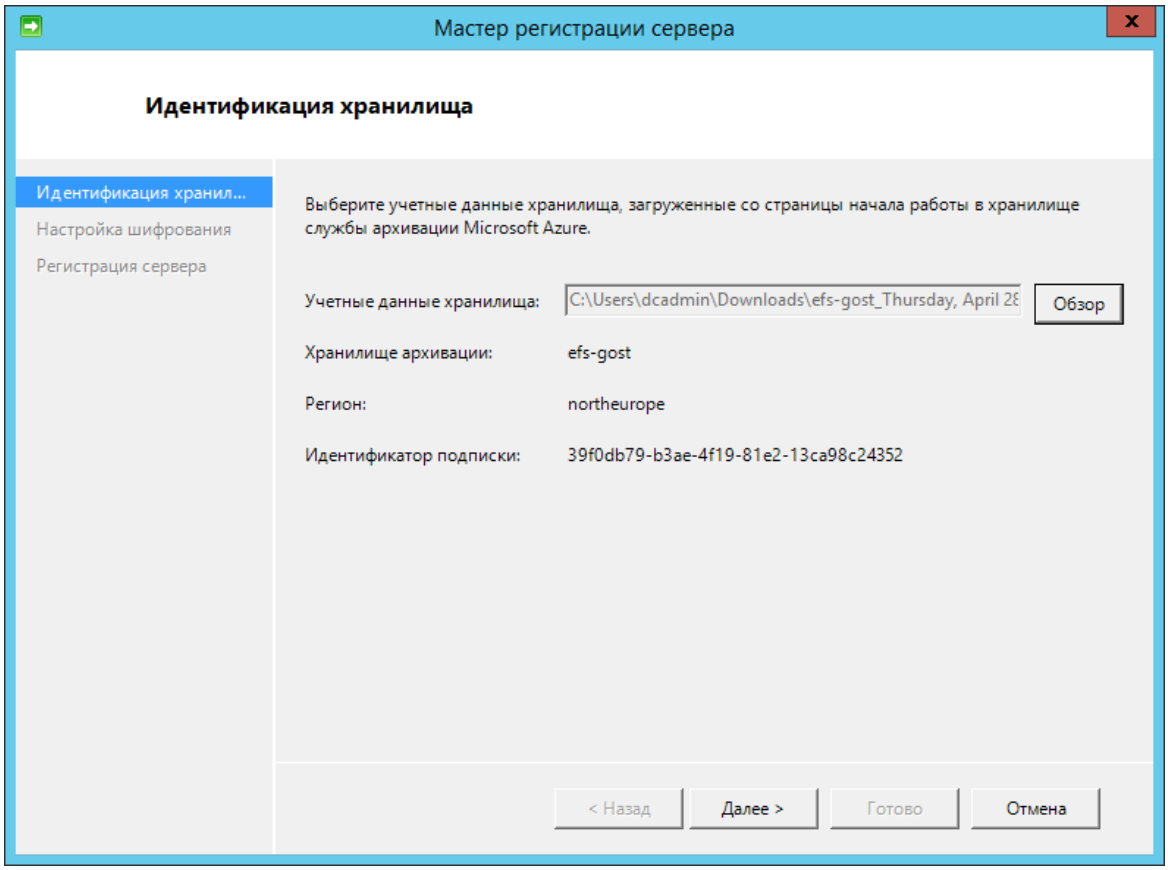
Установка Azure Backup Agent

Установите скачанный Azure Backup Agent с настройками по умолчанию. В ходе установки, при необходимости, будут установлены отсутствующие компоненты (.Net Framework, Powershell).

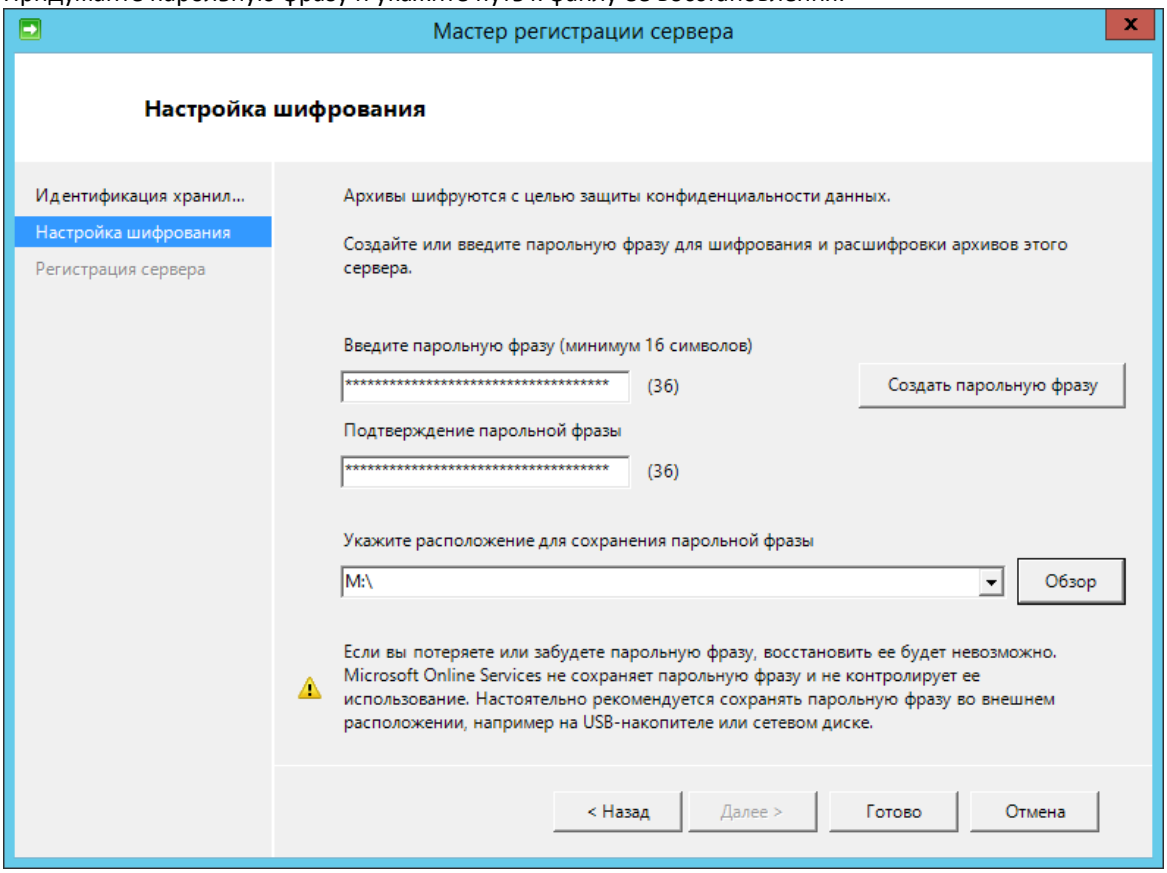
По завершении установки нажмите кнопку **Перейти к регистрации**



Отобразится следующее окно, выберите файл учетных данных, скачанный ранее.

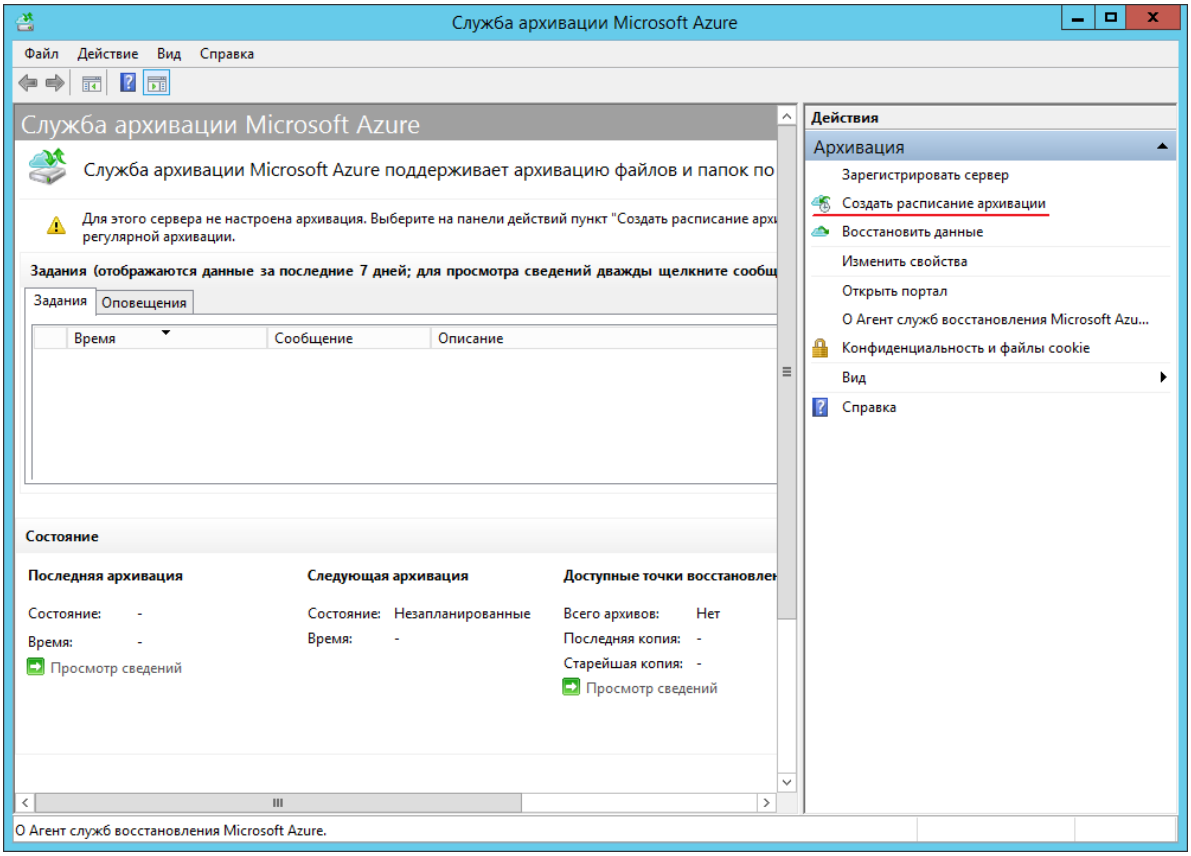


Придумайте парольную фразу и укажите путь к файлу ее восстановления.

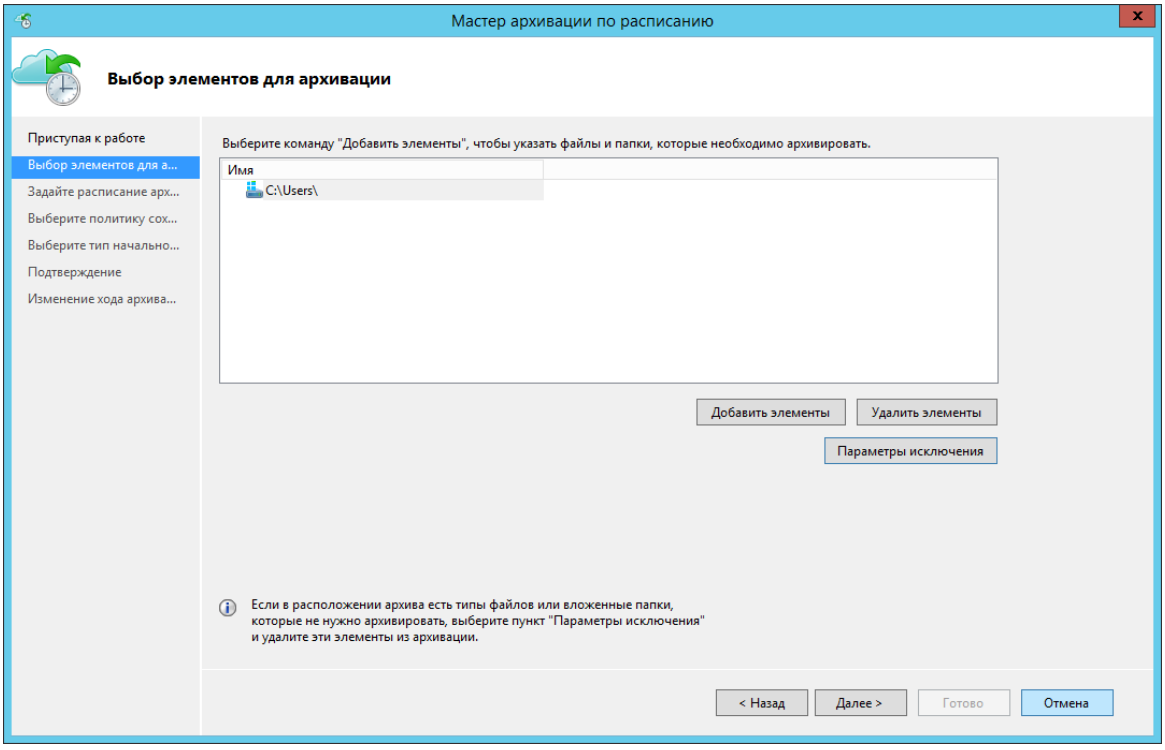


Настройка расписания резервирования

По завершении регистрации откроется окно **Служба архивации Microsoft Azure**. Создайте в нём расписание архивации.



В выборе элементов для архивации укажите папку с профилями пользователей.

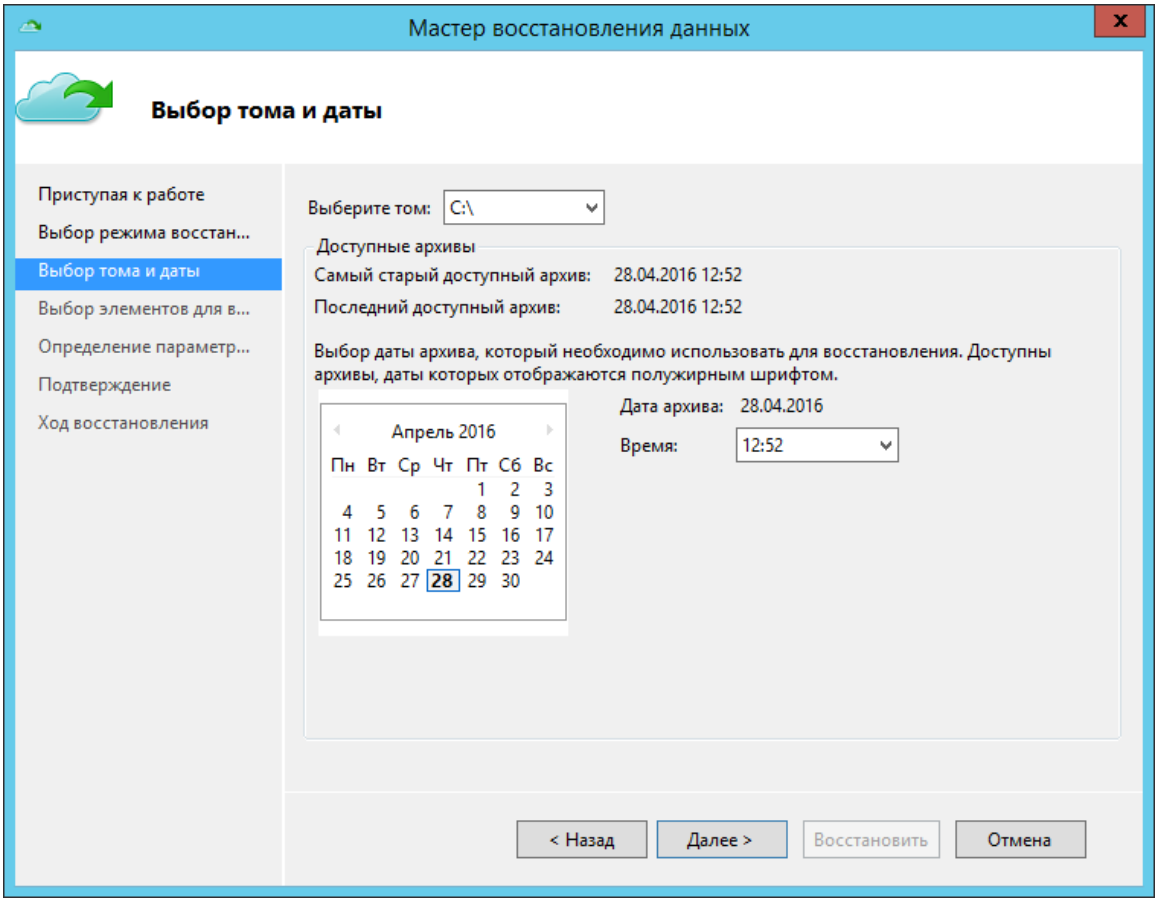


Остальные настройки оставьте по-умолчанию.

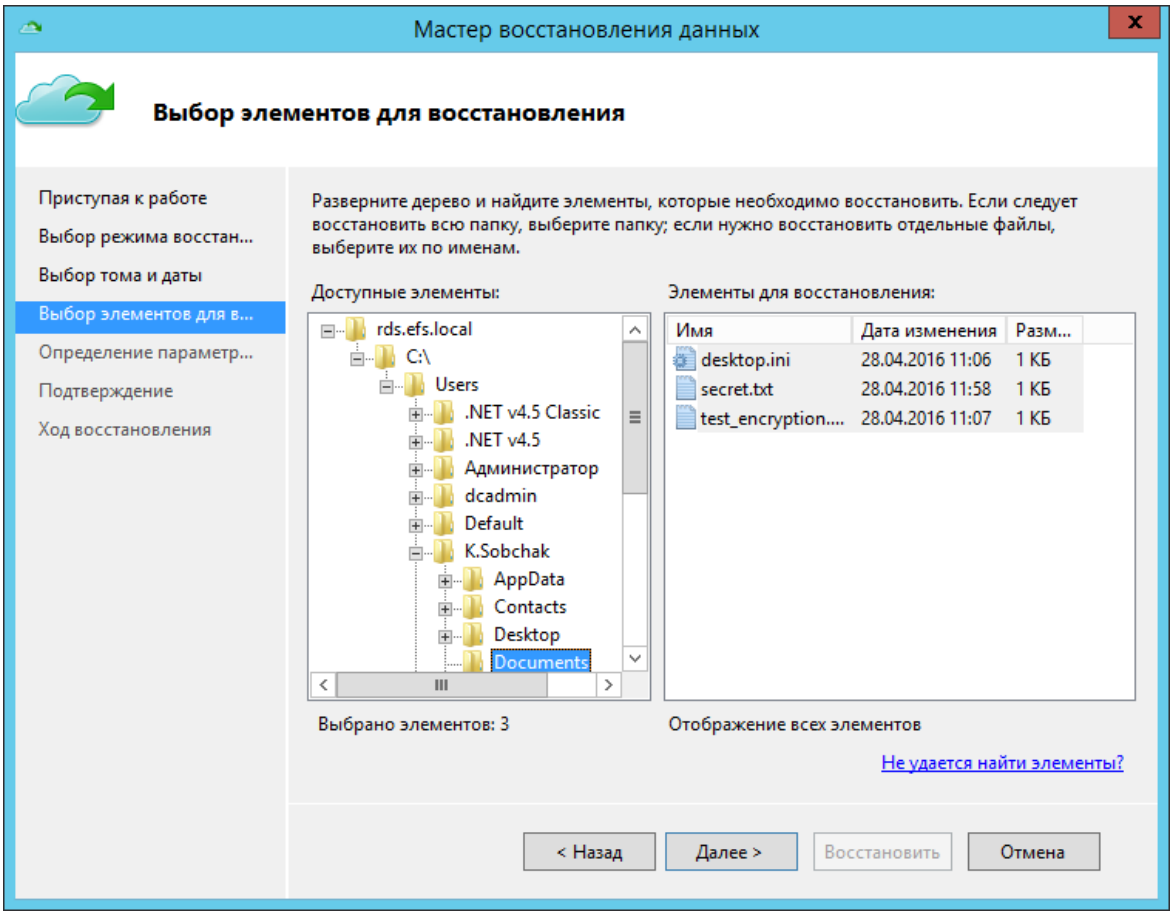
Для проверки настроек, нажмите **Выполнить мгновенную архивацию.**

Восстановление данных

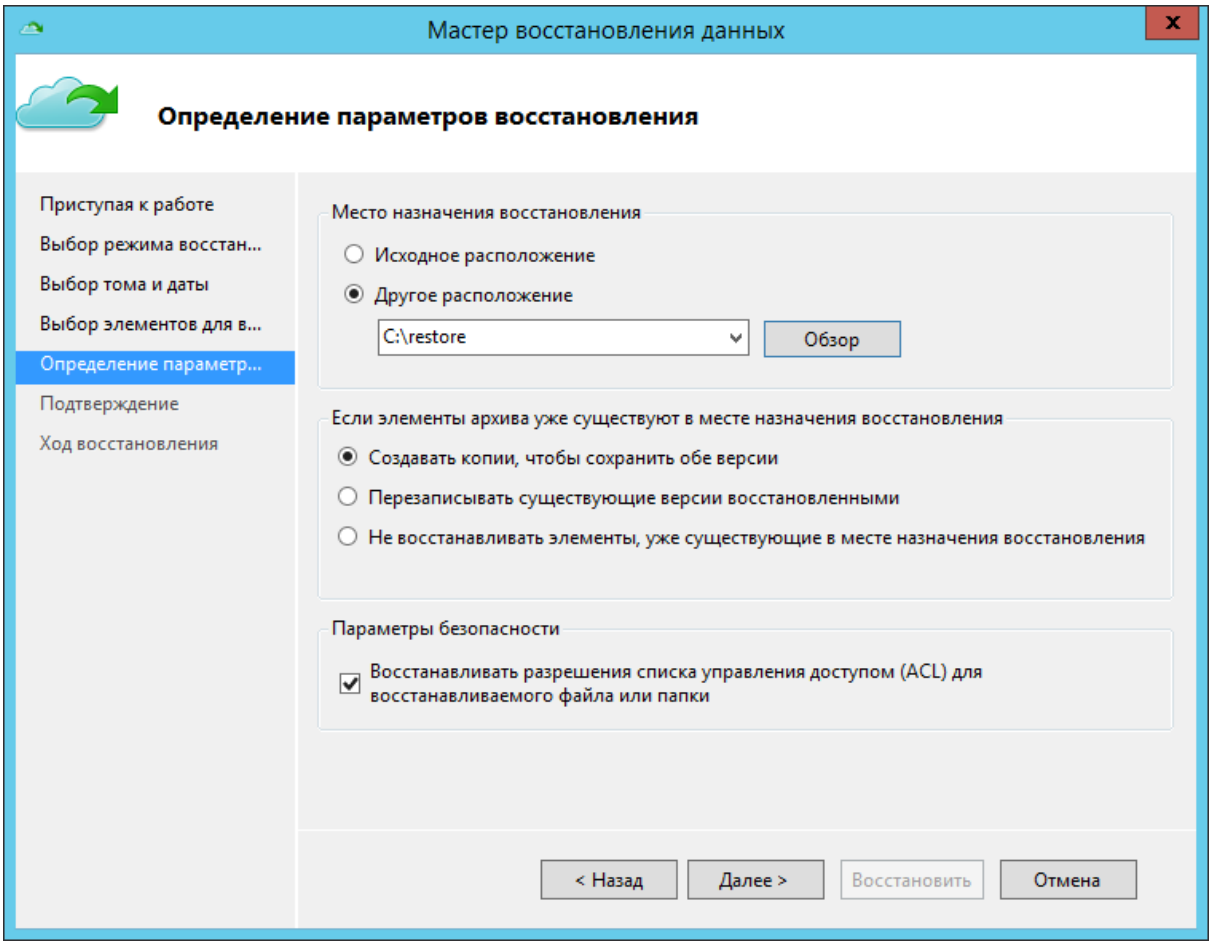
Восстановление из резервной копии выполняется аналогично.
Вызовите диалог восстановления данных, нажав кнопку **Восстановить данные.**
Выберите пункт **Этот сервер -> Обзор файлов -> Выбрать том и дату и время образа**



Далее выберите файлы для восстановления.



Выберите местоположение для восстанавливаемых файлов.



Проверить файлы может тот пользователя, который их зашифровал или при помощи агента восстановления **efsRA.**

Контакты, техническая поддержка

Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, компания «Аладдин Р. Д.».

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40.

Факс: +7 (495) 646-08-82.

E-mail: aladdin@aladdin-rd.ru (общий).

Web: www.aladdin-rd.ru

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

Техподдержка

Служба техподдержки принимает запросы только в письменном виде через веб-сайт:

www.aladdin-rd.ru/support/index.php

Для оперативного решения вашей проблемы укажите используемый Вами продукт, его версию, подробно опишите условия и сценарии применения, по возможности, снабдите сообщение снимками экрана, примерами исходного кода.

Регистрация изменений

Версия	Изменения
1.0	Исходная версия документа

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12
Лицензии ФСБ России № 12632 Н от 20.12.12, № 24530 от 25.02.14
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15
Microsoft Silver OEM Hardware Partner, Microsoft Silver Cloud Platform Partner, Apple Developer

Тел. +7 (495) 223-00-01 Email: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru