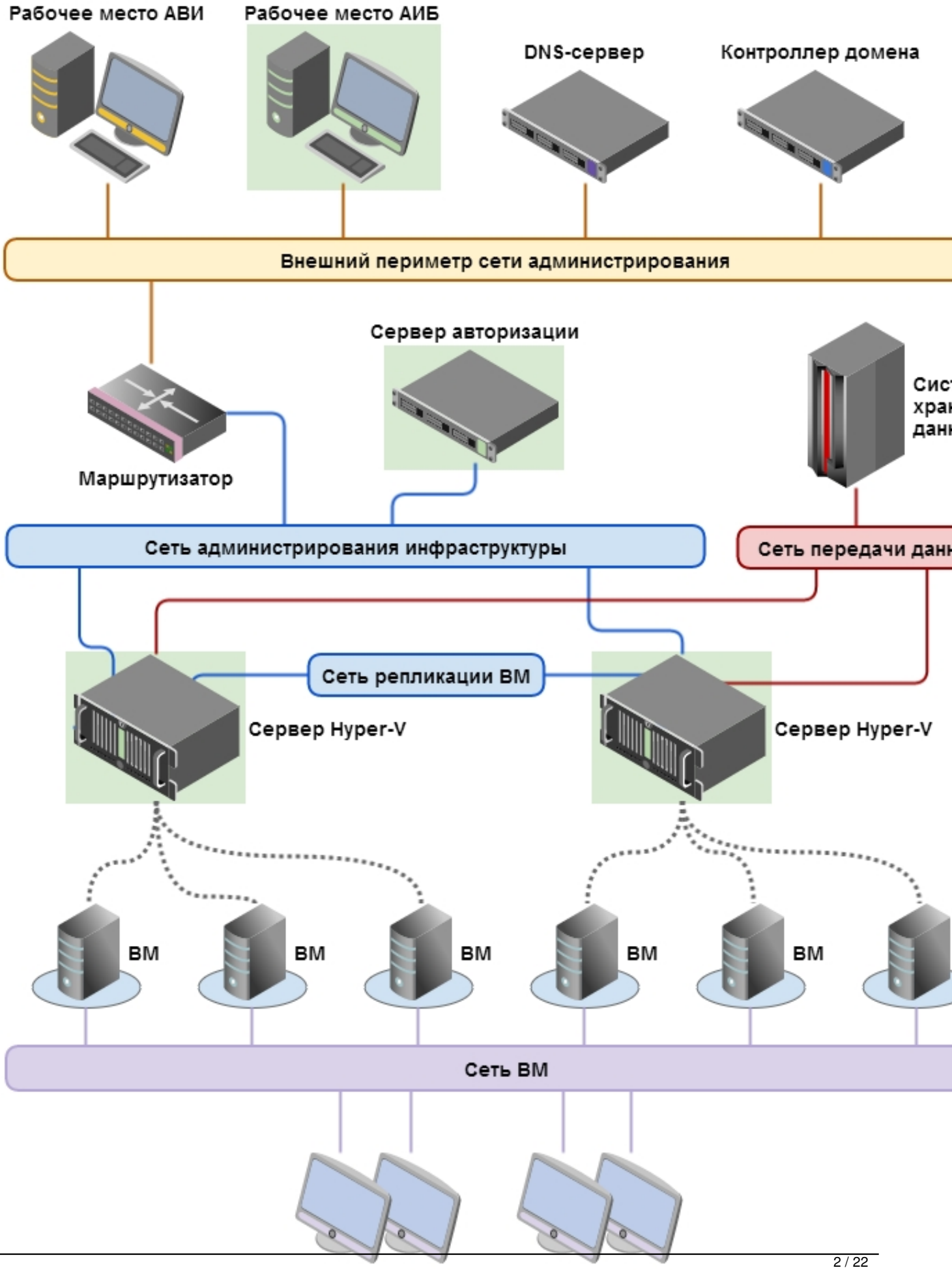
Эксплуатация решения vGate R2 for Hyper-V с точки зрения администратора

Автор: Александр Самойленко
Дата: 27/12/2014

В прошлых статьях мы рассказывали о продукте vGate R2 for Hyper-V , который позволяет проводить защищенную аутентификацию администраторов, разграничивать доступ к различным объектам инфраструктуры и проводить аудит событий безопасности. О возможностях этого продукта мы писали тут , о настройке - тут и тут , а сегодня мы поговорим о том, как выглядит повседневная эксплуатация решения со стороны администратора ИБ, который является также и администратором решения vGate.

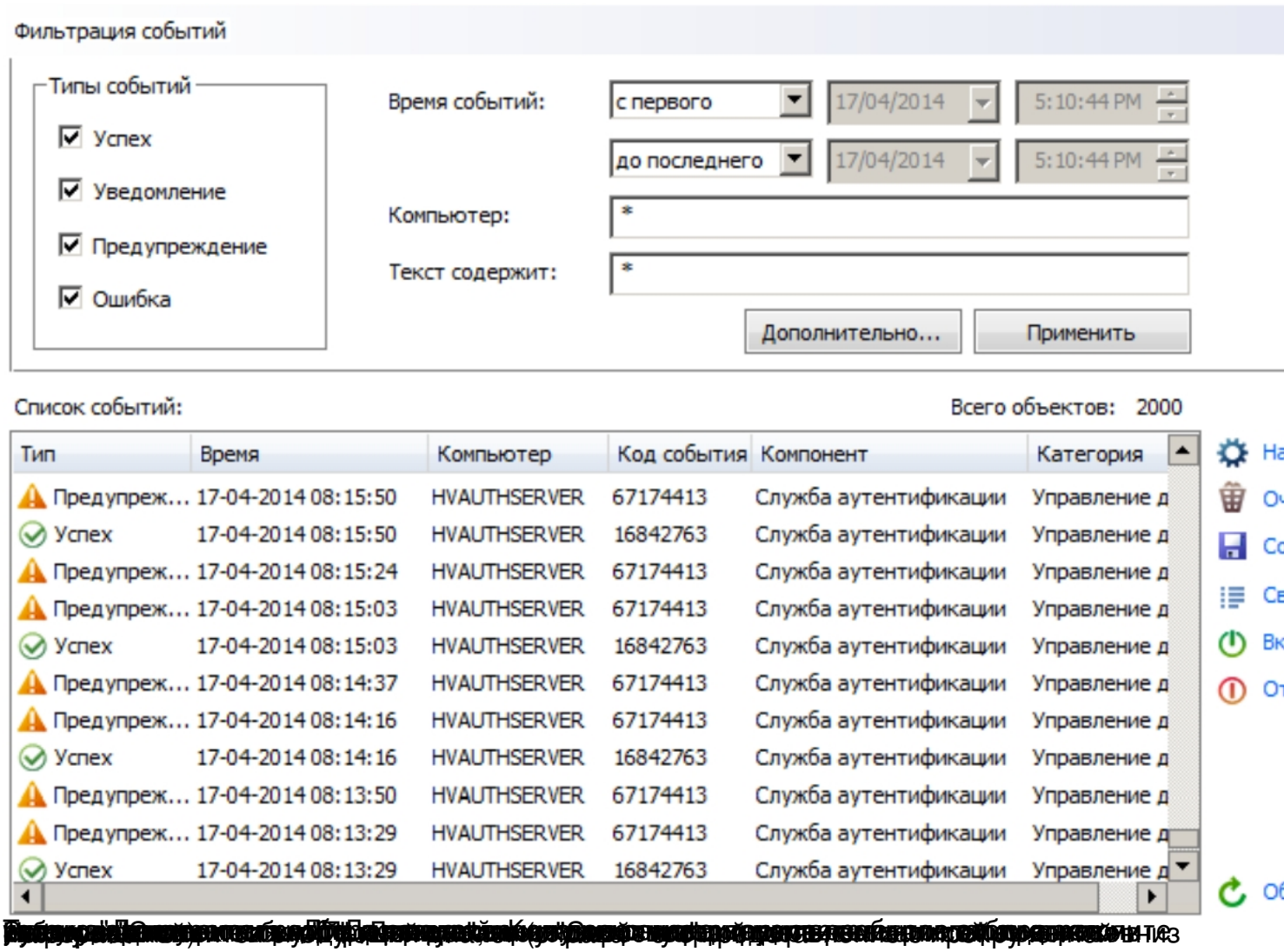
Итак, приведем сначала референсную архитектуру vGate R2 для инфраструктуры Hyper-V, к которой можно обращаться по ходу чтения статьи:

Автор:
27.12.14 20:10 -



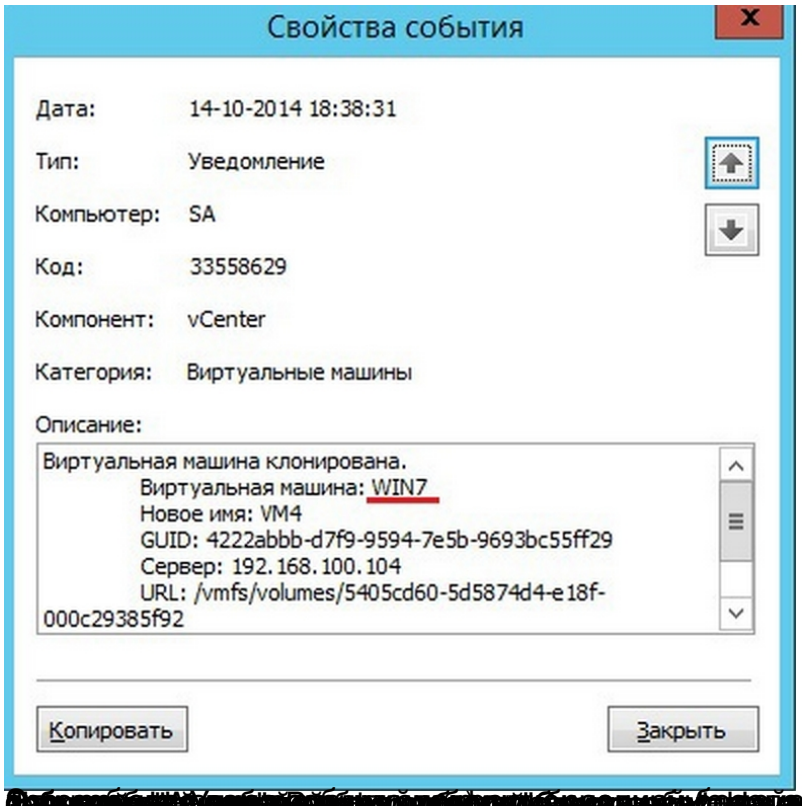
Автор:
27.12.14 20:10 -

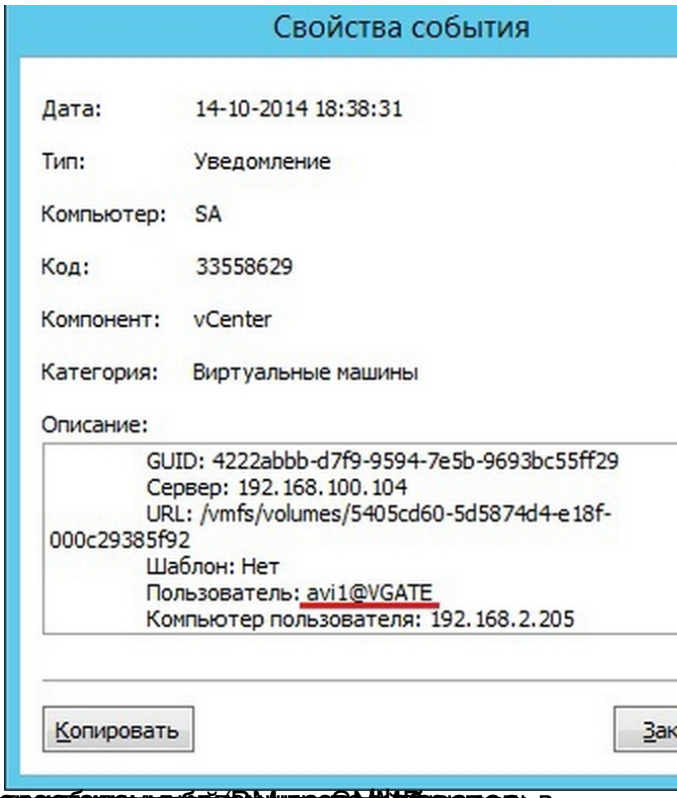
[redacted]



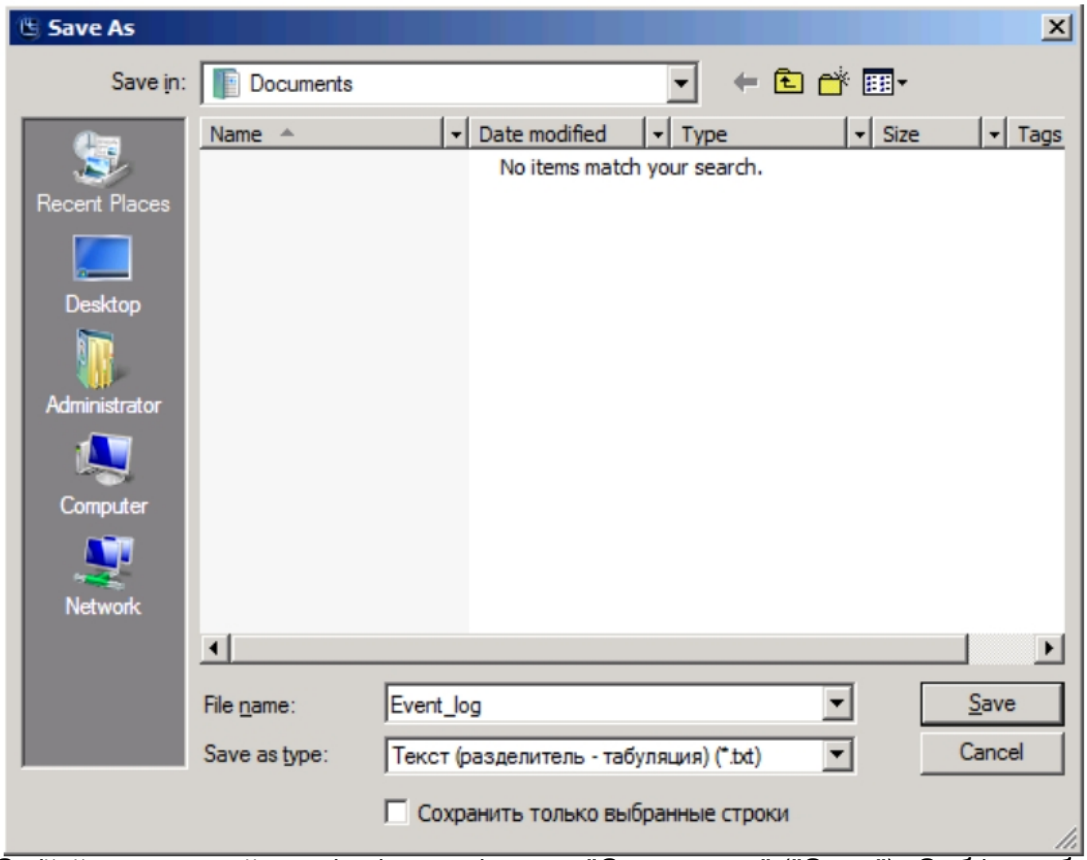
[redacted]

Автор:
27.12.14 20:10 -



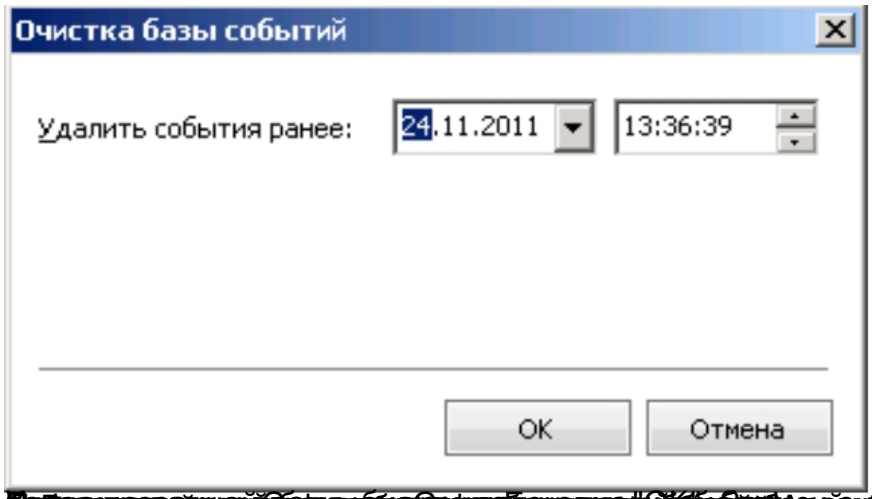


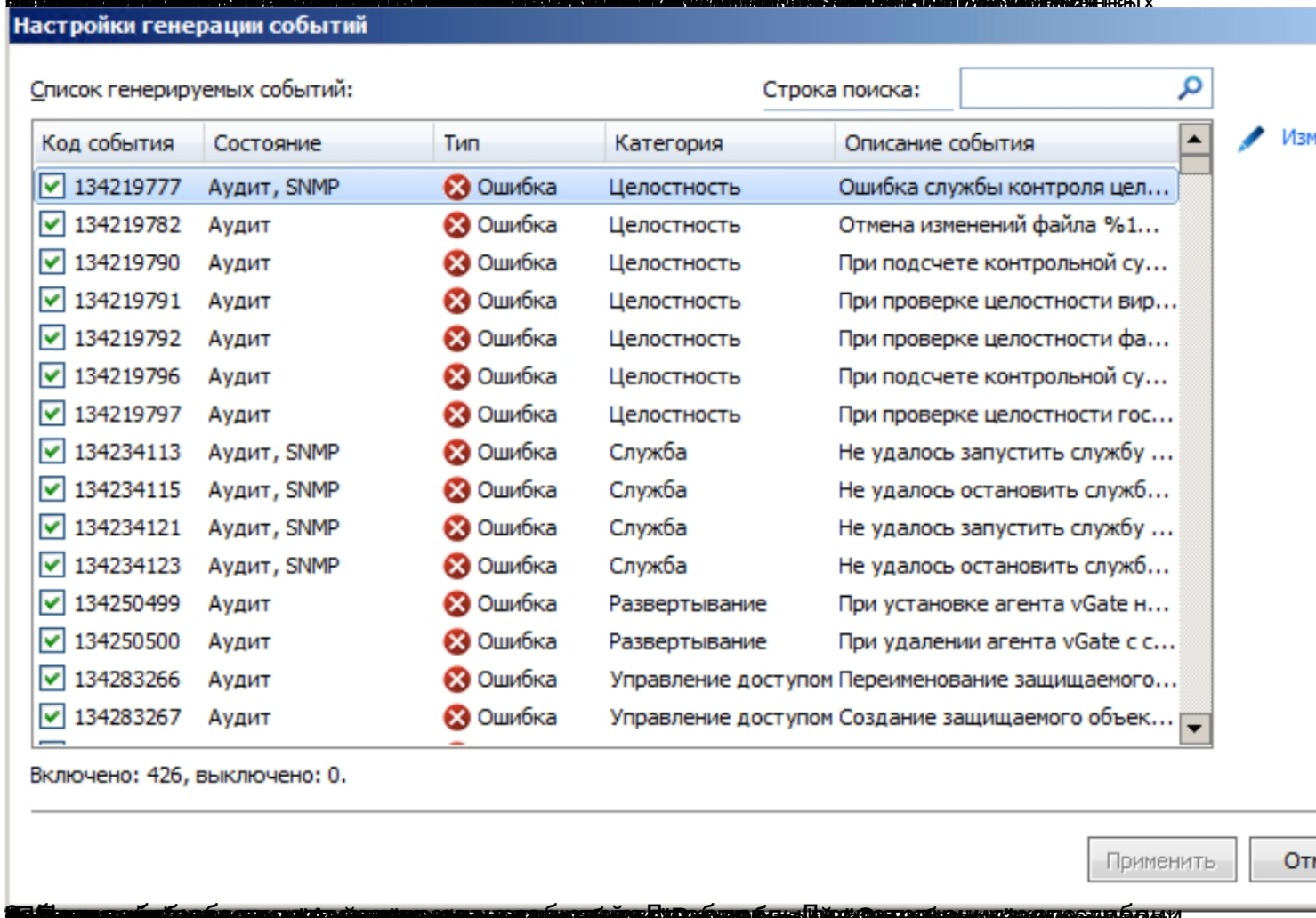
в

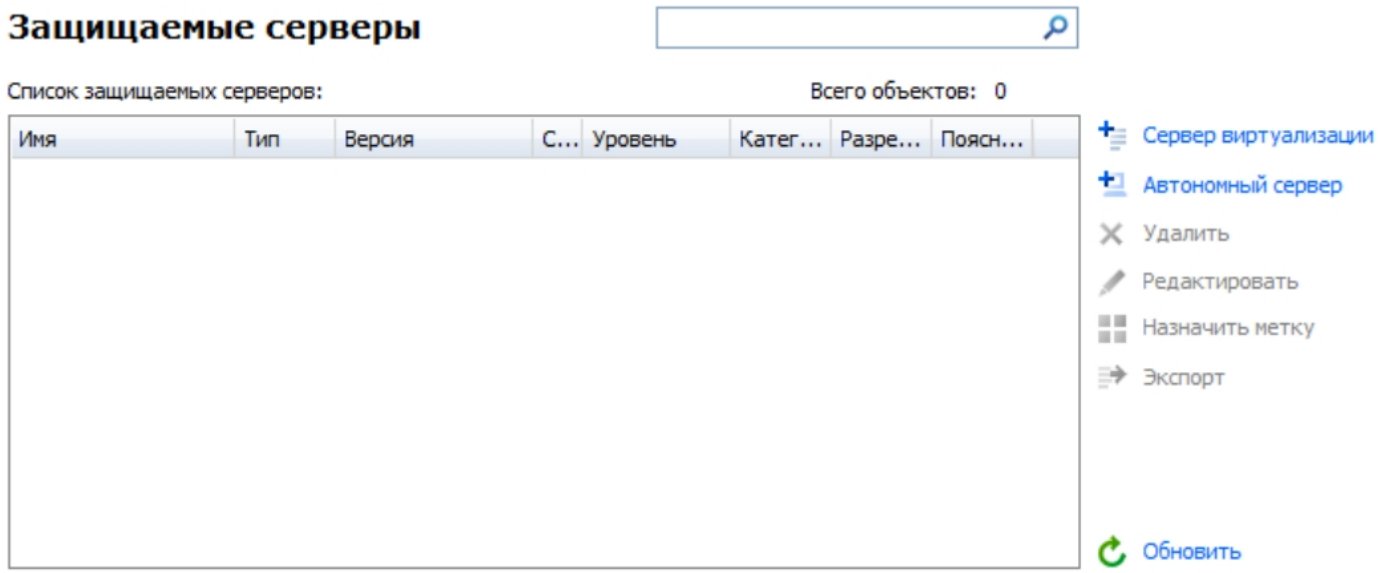


в

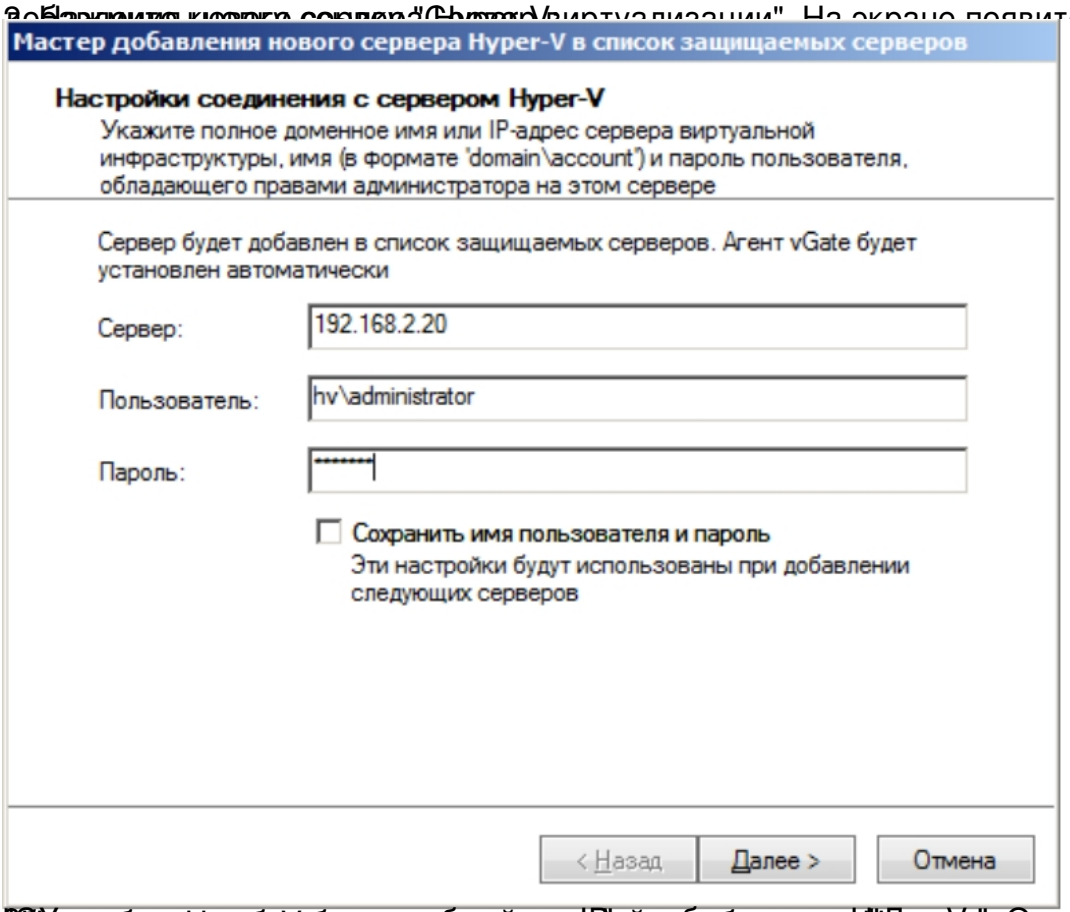
Автор:
27.12.14 20:10 -





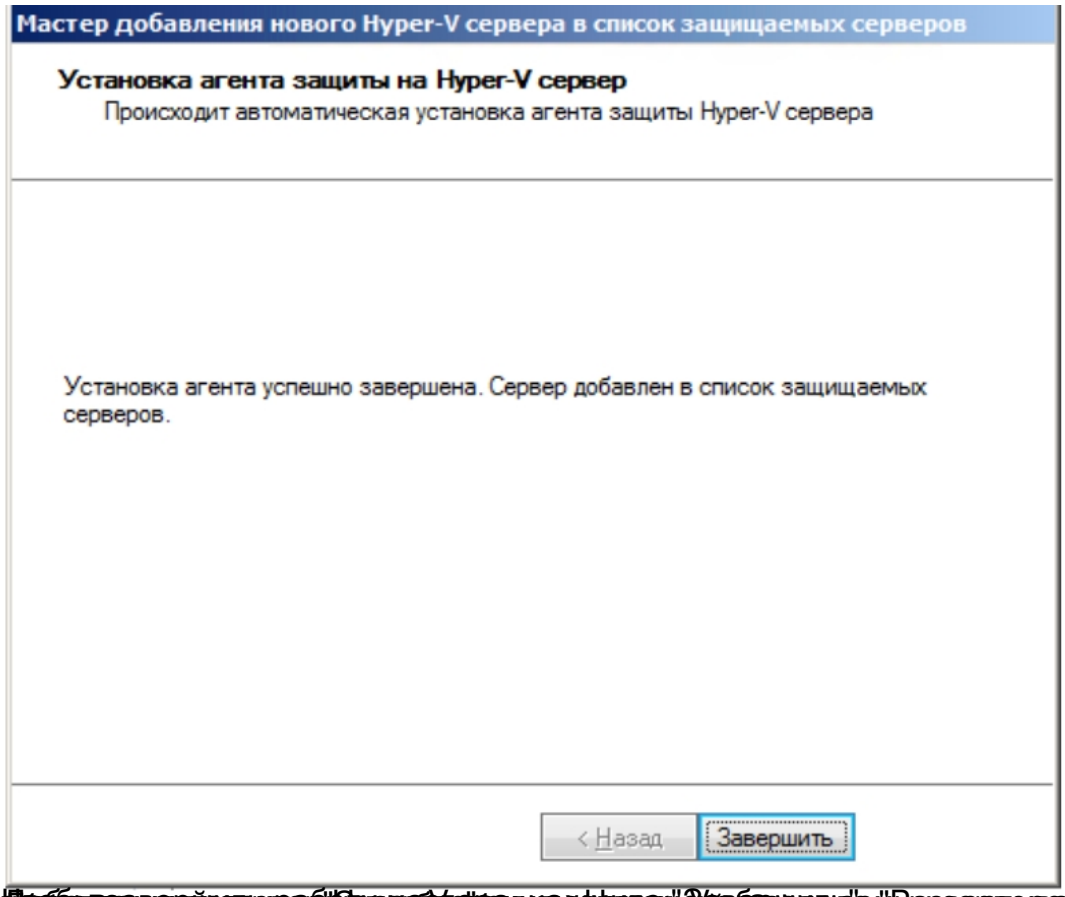


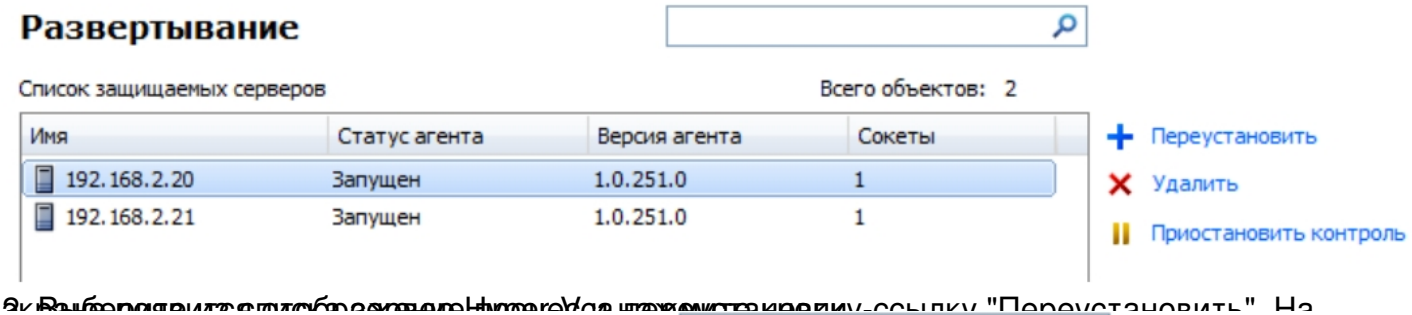
Добавление нового сервера виртуализации". На экране появится мастер

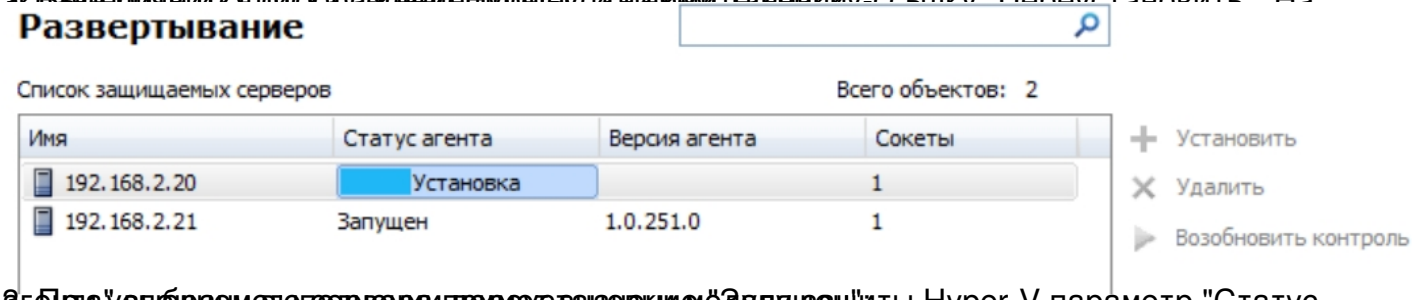


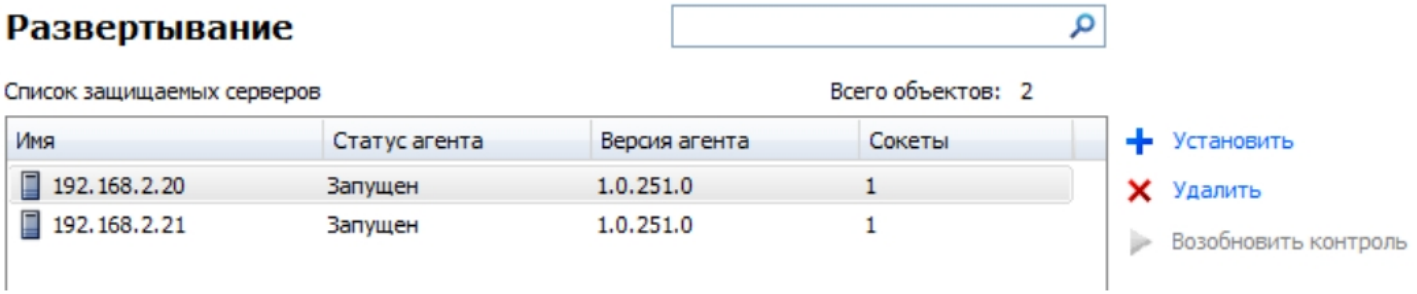
Обратите внимание, что

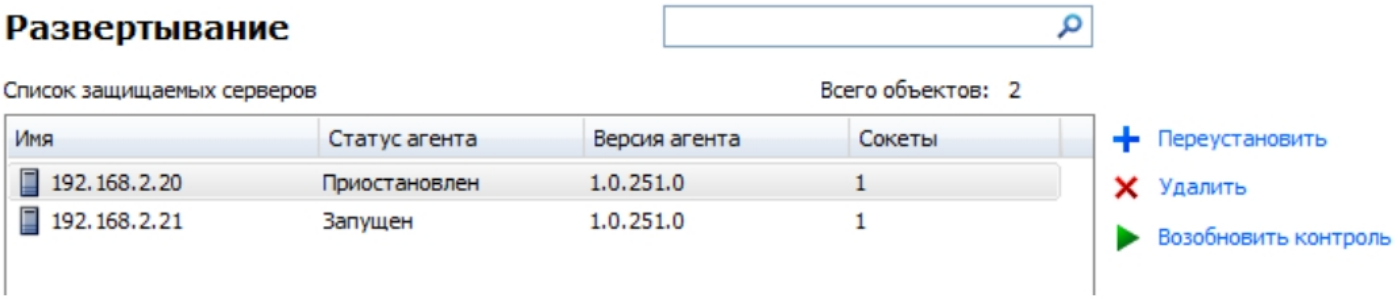
Автор:
27.12.14 20:10 -

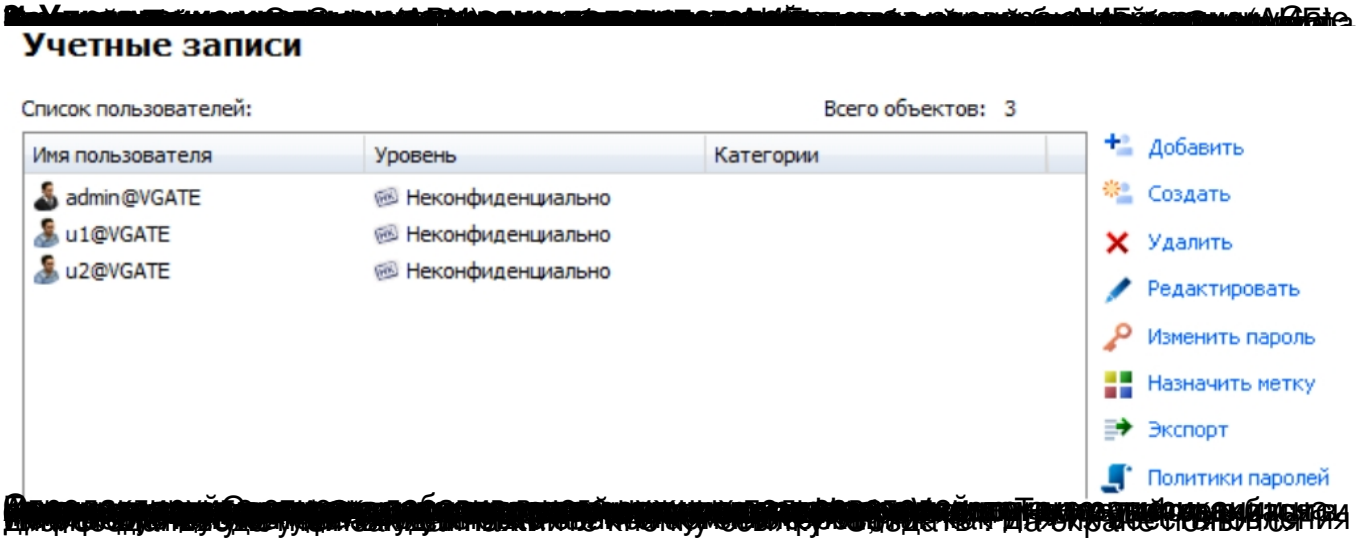




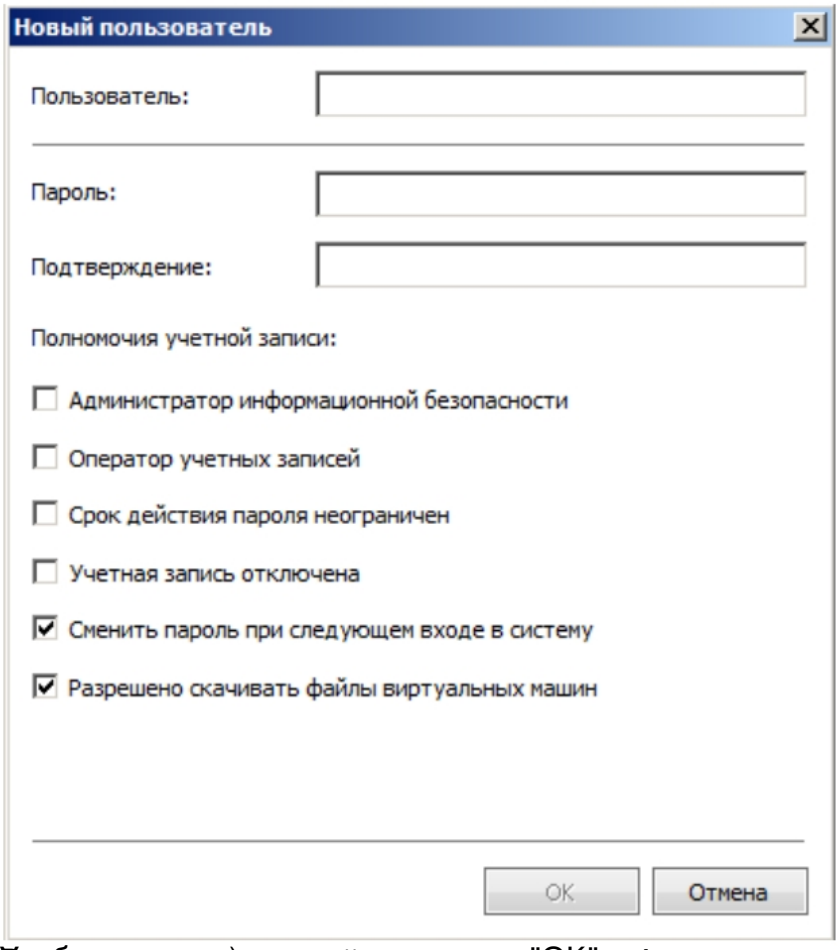



Развертывание
Список защищаемых серверов
Всего объектов: 2
Имя
Статус агента
Версия агента
Сокеты
192.168.2.20
Запущен
1.0.251.0
1
192.168.2.21
Запущен
1.0.251.0
1
Установить
Удалить
Возобновить контроль

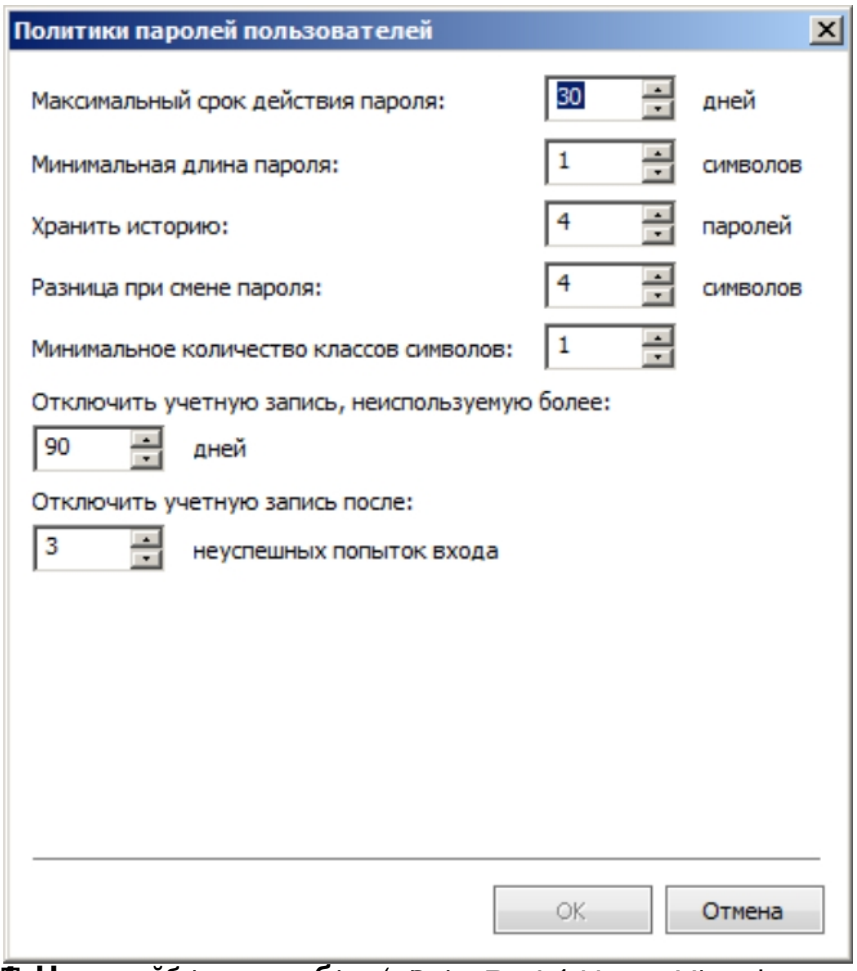

Развертывание
Список защищаемых серверов
Всего объектов: 2
Имя
Статус агента
Версия агента
Сокеты
192.168.2.20
Приостановлен
1.0.251.0
1
192.168.2.21
Запущен
1.0.251.0
1
Переустановить
Удалить
Возобновить контроль


Учетные записи
Список пользователей:
Всего объектов: 3
Имя пользователя
Уровень
Категории
admin@VGATE
Неконфиденциально
u1@VGATE
Неконфиденциально
u2@VGATE
Неконфиденциально
Добавить
Создать
Удалить
Редактировать
Изменить пароль
Назначить метку
Экспорт
Политики паролей

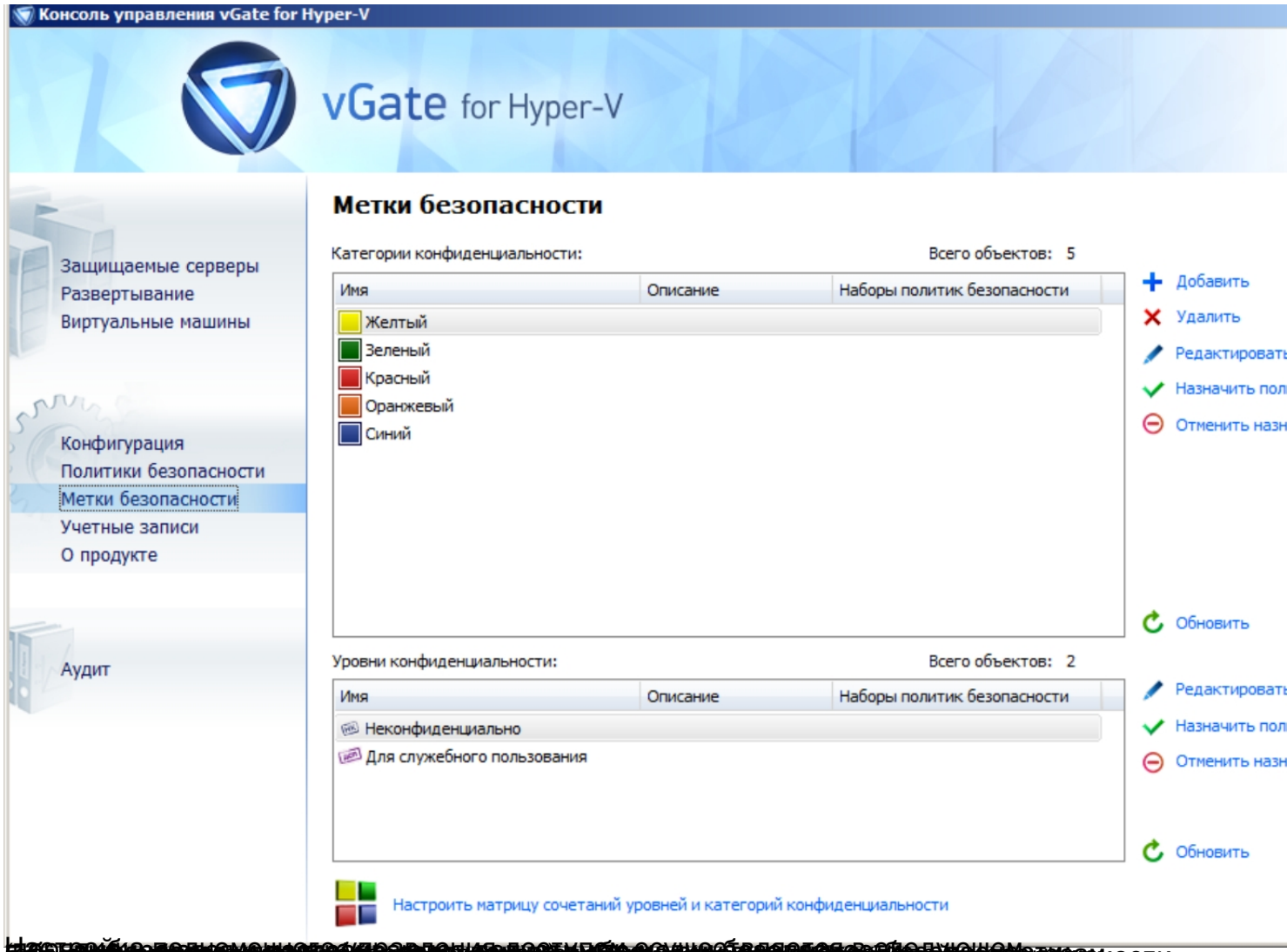
Автор:
27.12.14 20:10 -



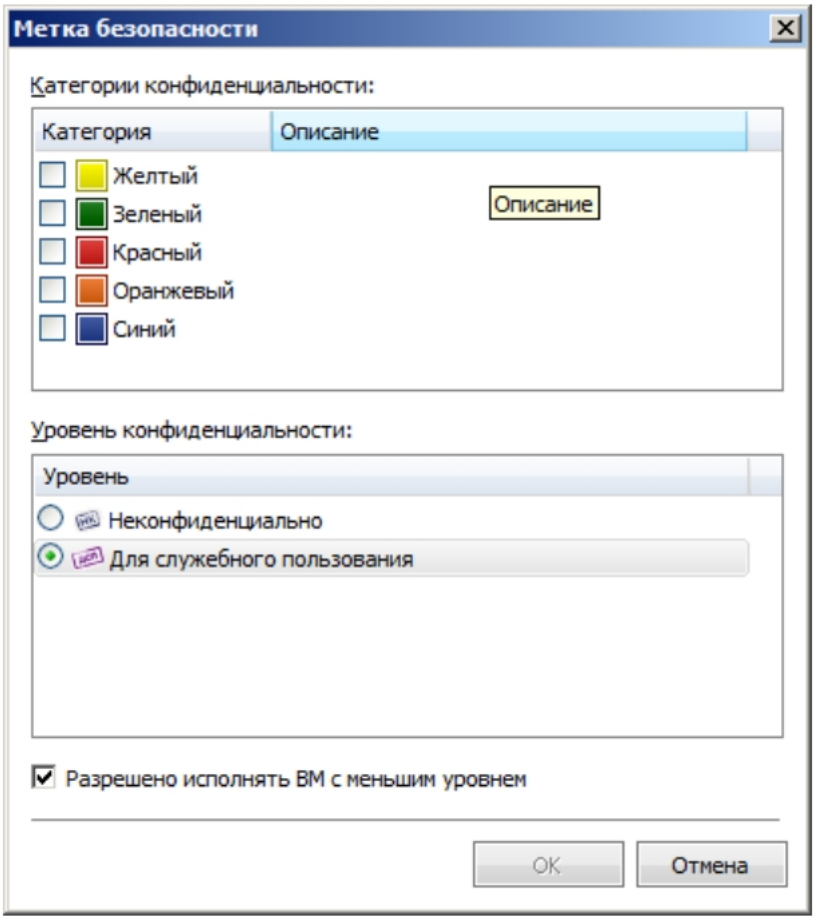
Автор:
27.12.14 20:10 -



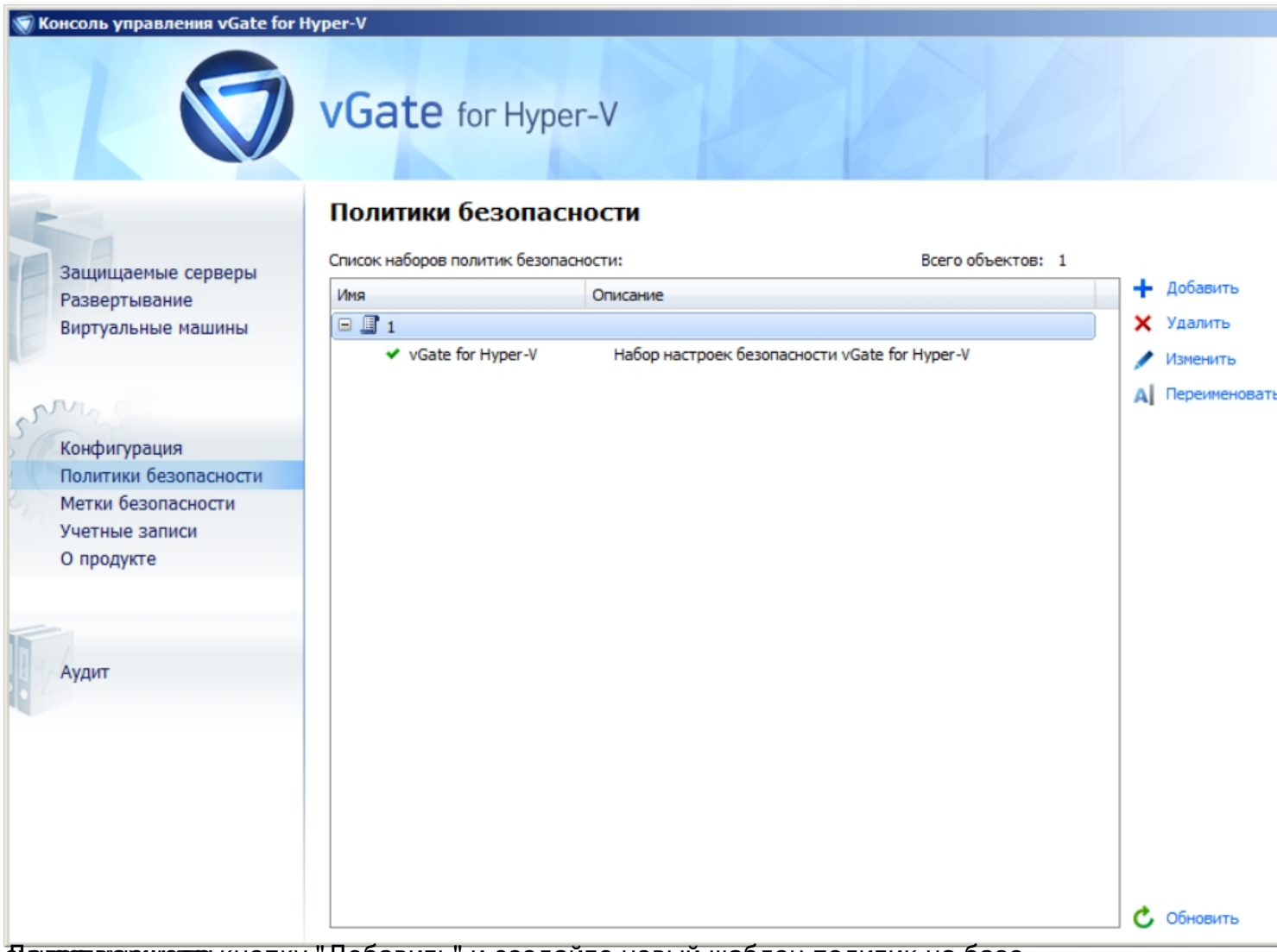
Автор:
27.12.14 20:10 -



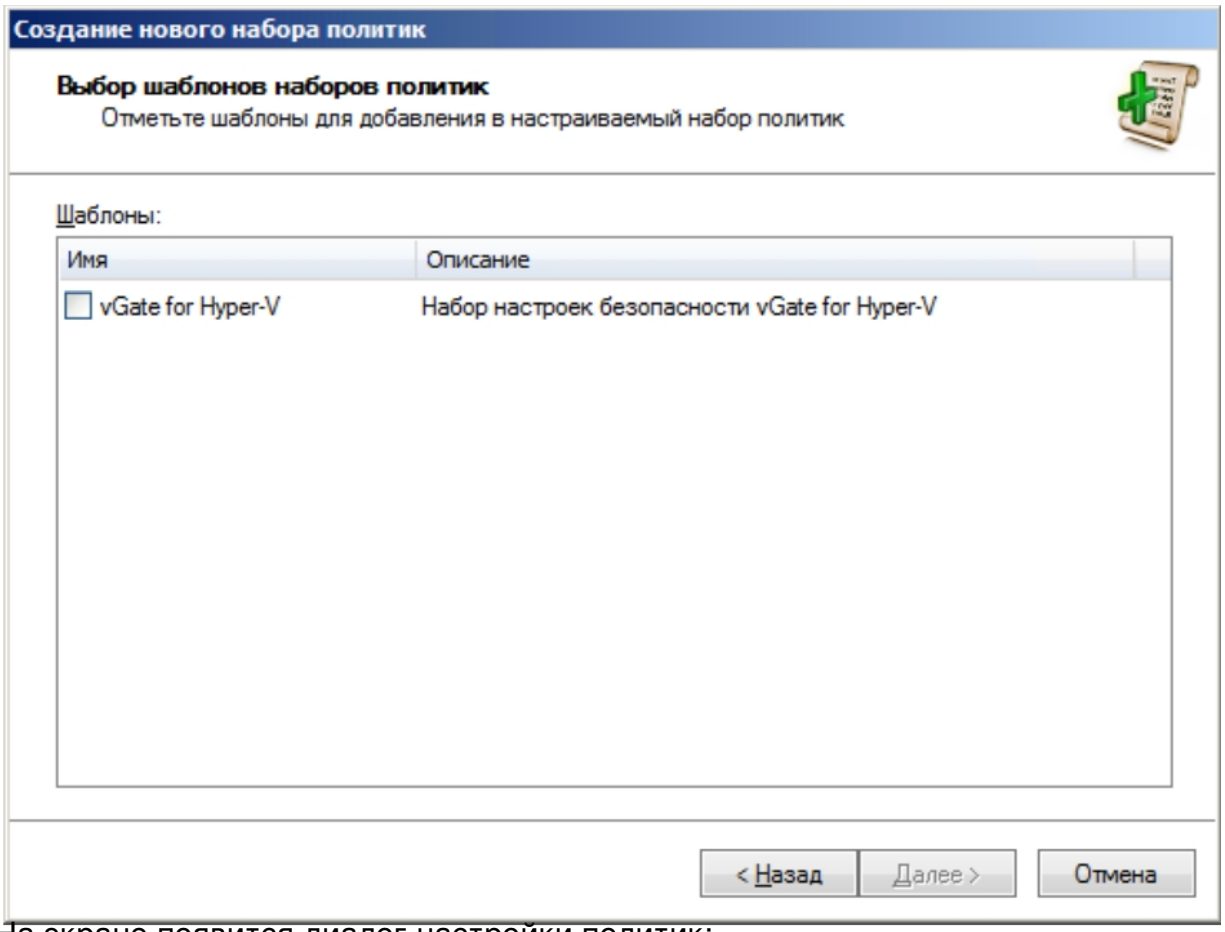
Автор:
27.12.14 20:10 -



Автор:
27.12.14 20:10 -

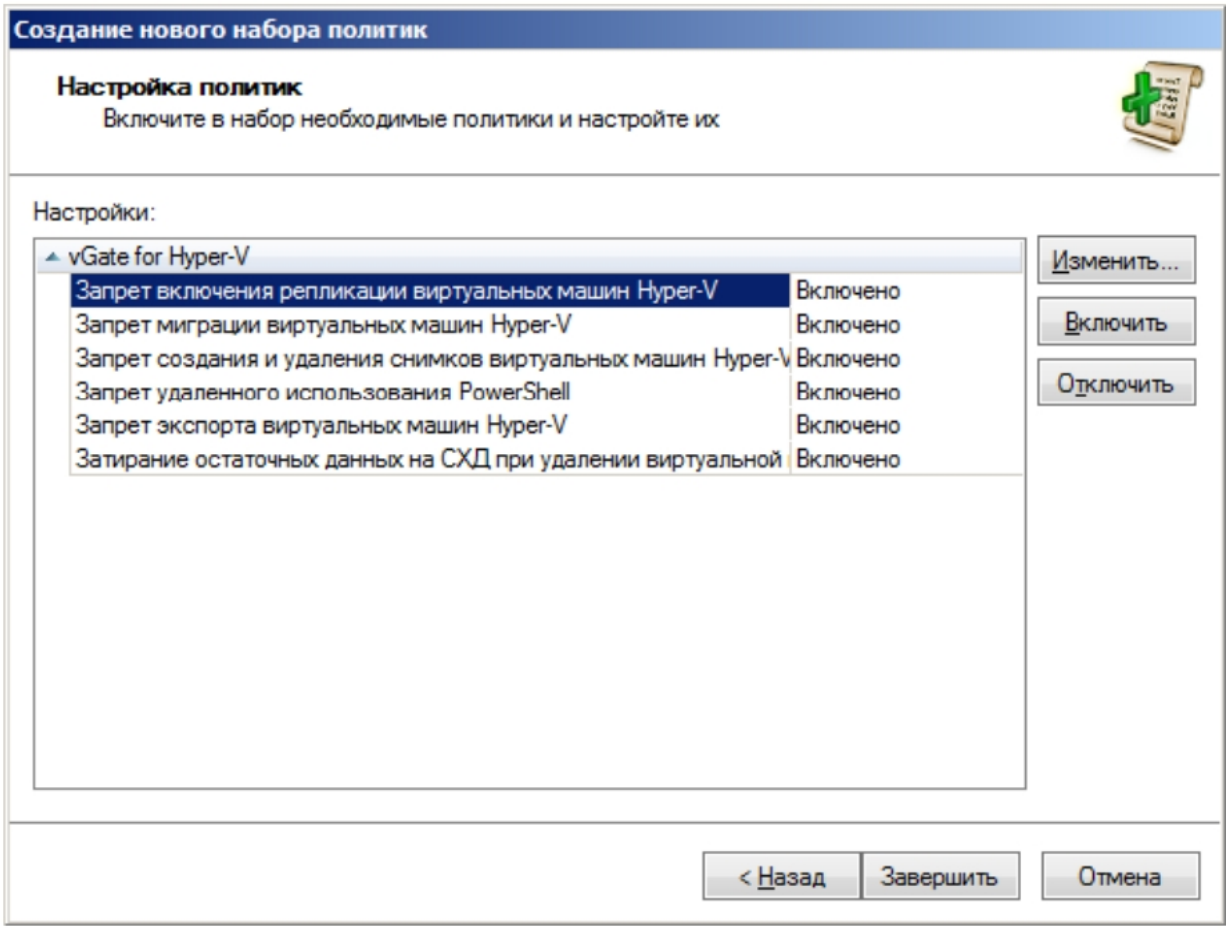


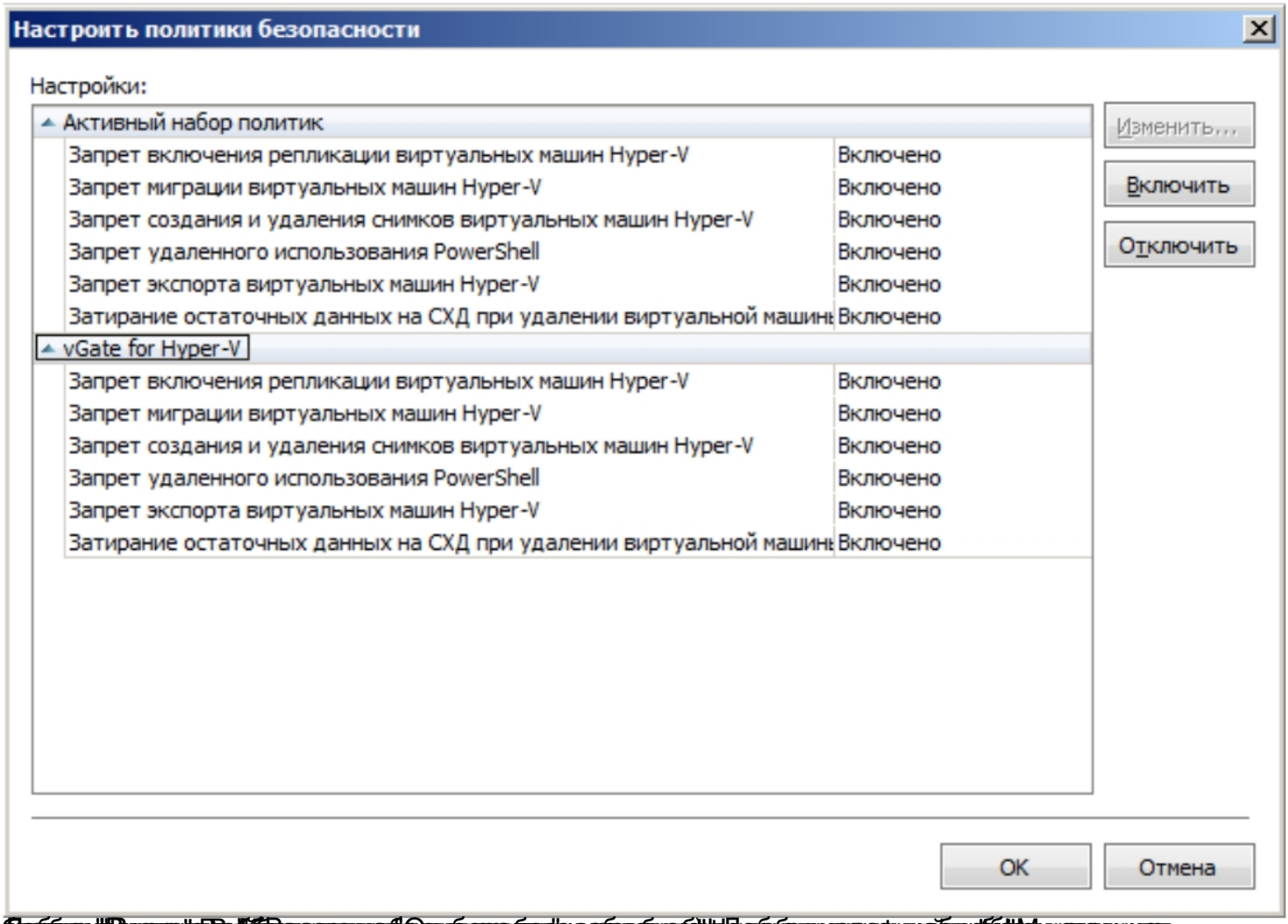
Далее нужно нажать кнопку "Добавить" и создайте новый шаблон политик на базе



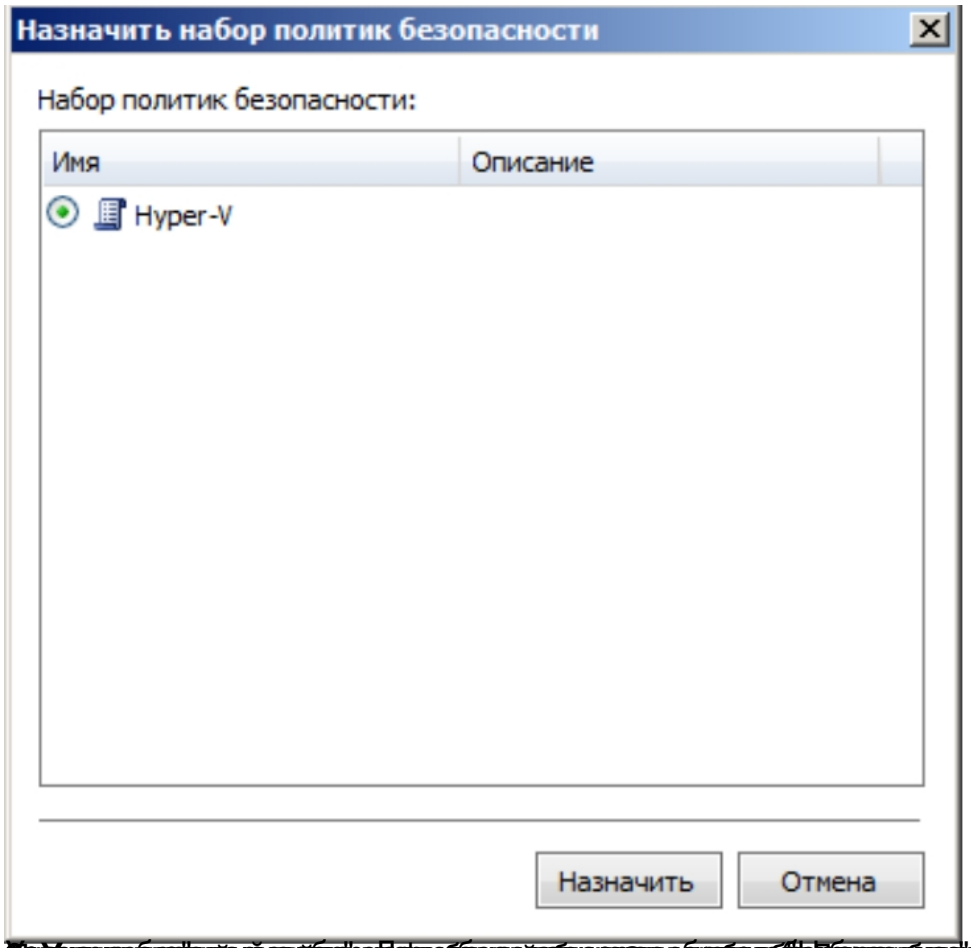
На экране появится диалог настройки политик:

Автор:
27.12.14 20:10 -

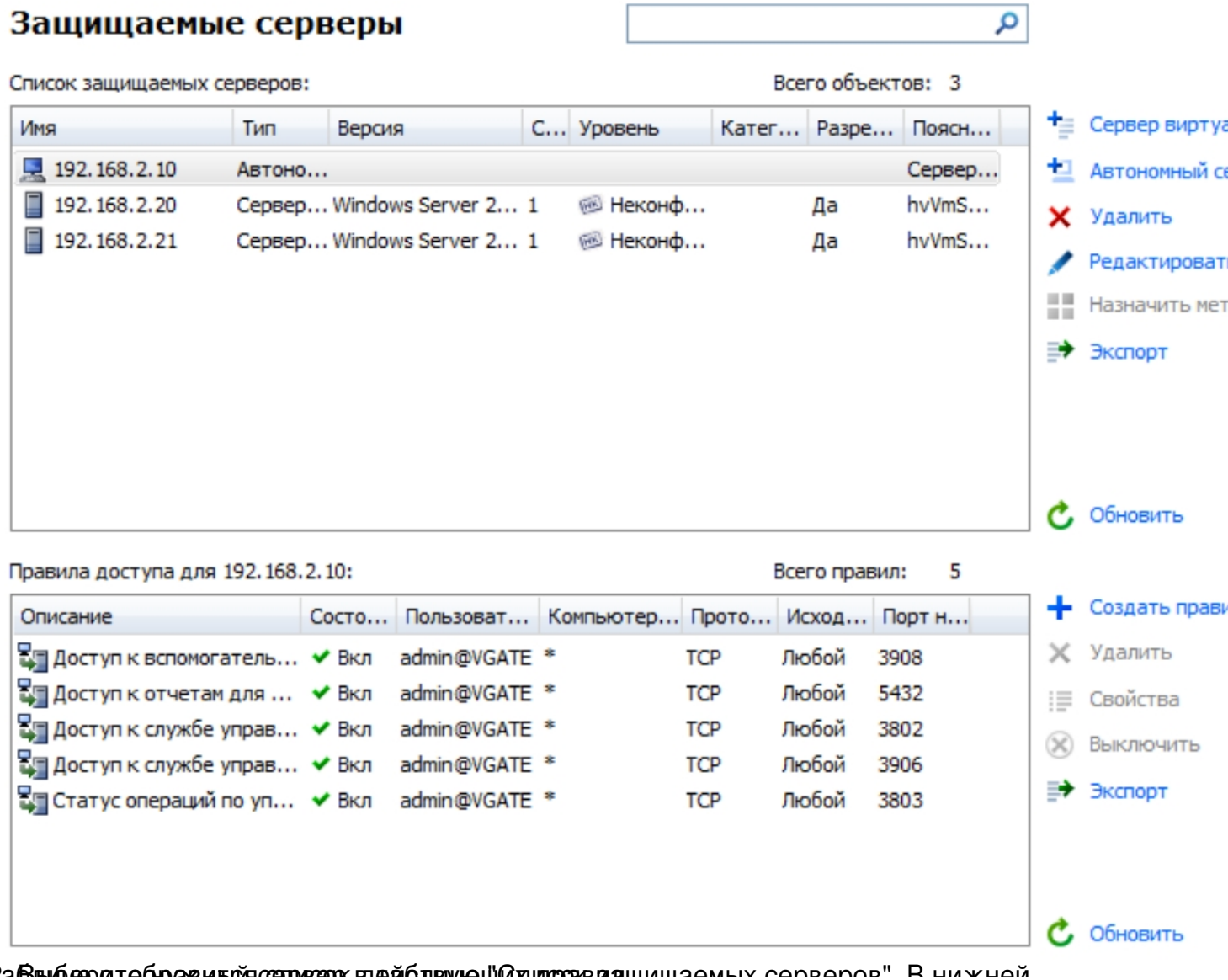



Настроить политики безопасности
Настройки:
Активный набор политик
Запрет включения репликации виртуальных машин Hyper-V Включено
Запрет миграции виртуальных машин Hyper-V Включено
Запрет создания и удаления снимков виртуальных машин Hyper-V Включено
Запрет удаленного использования PowerShell Включено
Запрет экспорта виртуальных машин Hyper-V Включено
Затирание остаточных данных на СХД при удалении виртуальной машины Включено
vGate for Hyper-V
Запрет включения репликации виртуальных машин Hyper-V Включено
Запрет миграции виртуальных машин Hyper-V Включено
Запрет создания и удаления снимков виртуальных машин Hyper-V Включено
Запрет удаленного использования PowerShell Включено
Запрет экспорта виртуальных машин Hyper-V Включено
Затирание остаточных данных на СХД при удалении виртуальной машины Включено
Изменить...
Включить
Отключить
OK
Отмена

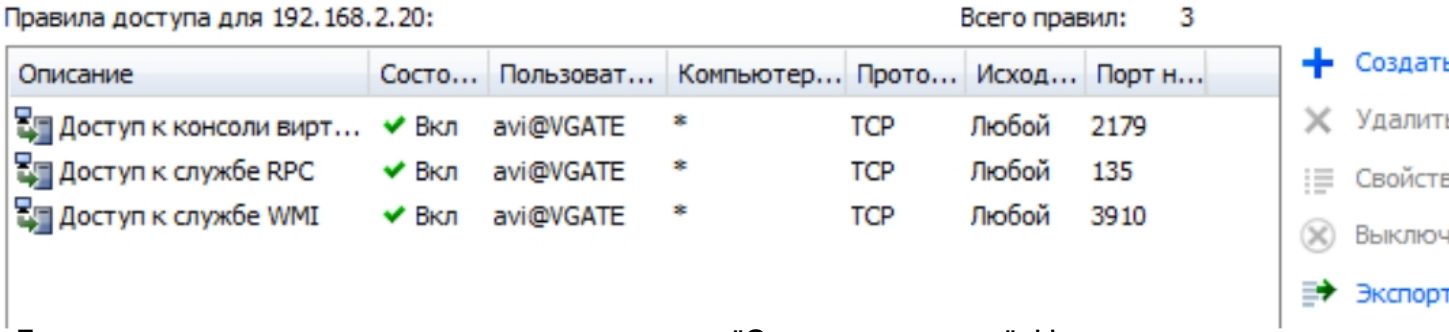
Автор:
27.12.14 20:10 -



Автор:
27.12.14 20:10 -

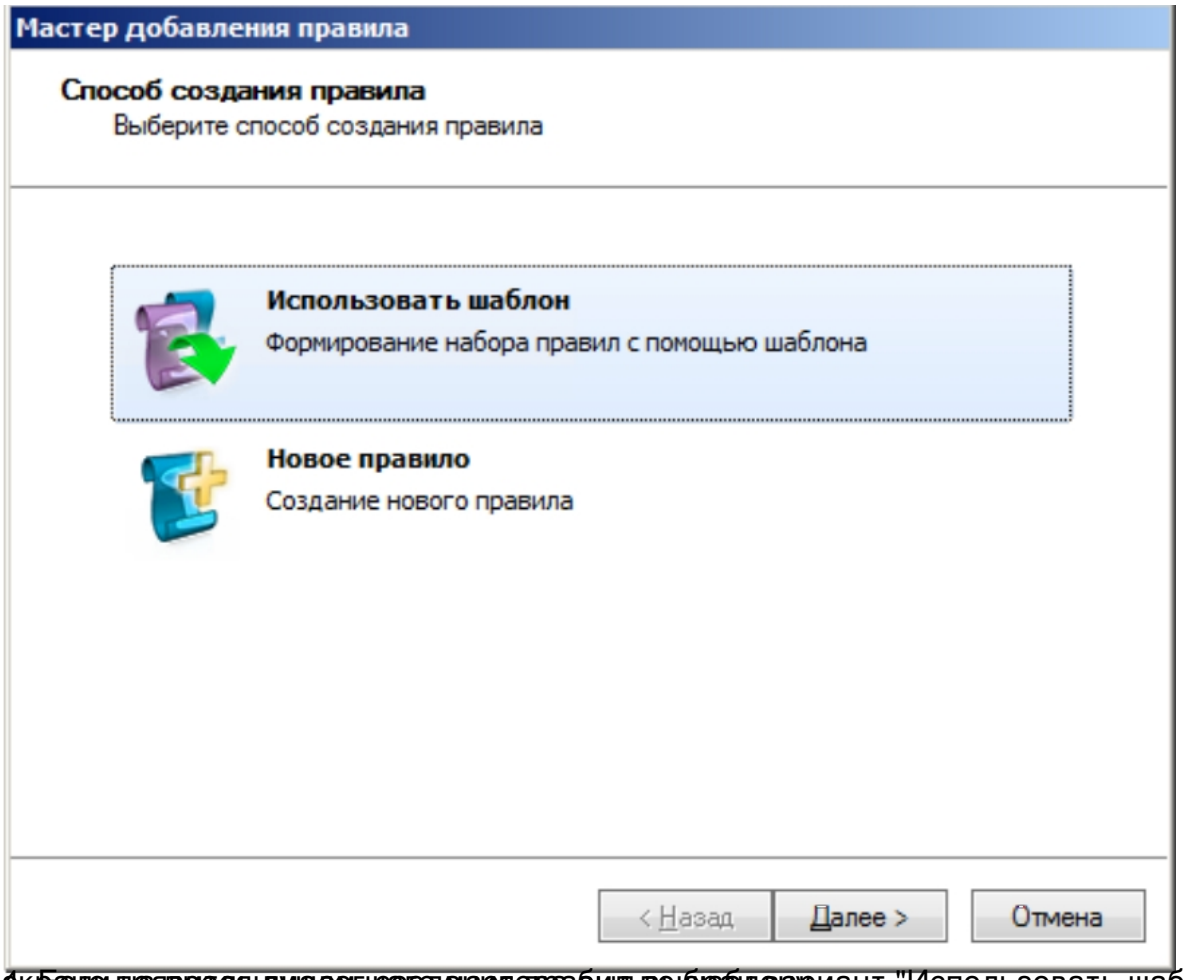


3. Выберите требуемый сервер в списке "Список защищаемых серверов". В нижней части окна отобразится список правил доступа для выбранного сервера.

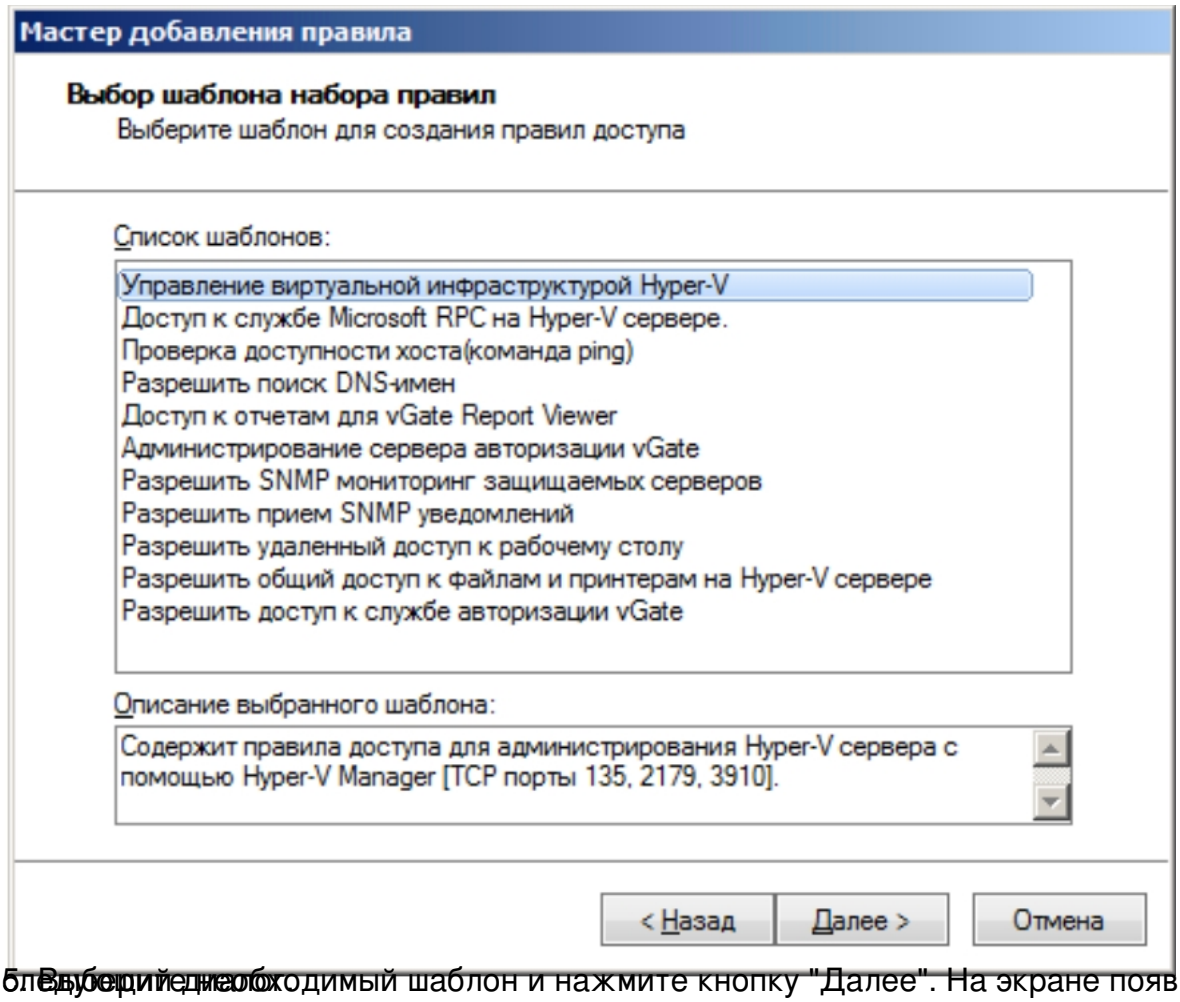


4. Для создания нового правила нажмите кнопку-ссылку "Создать правило". На экране появится

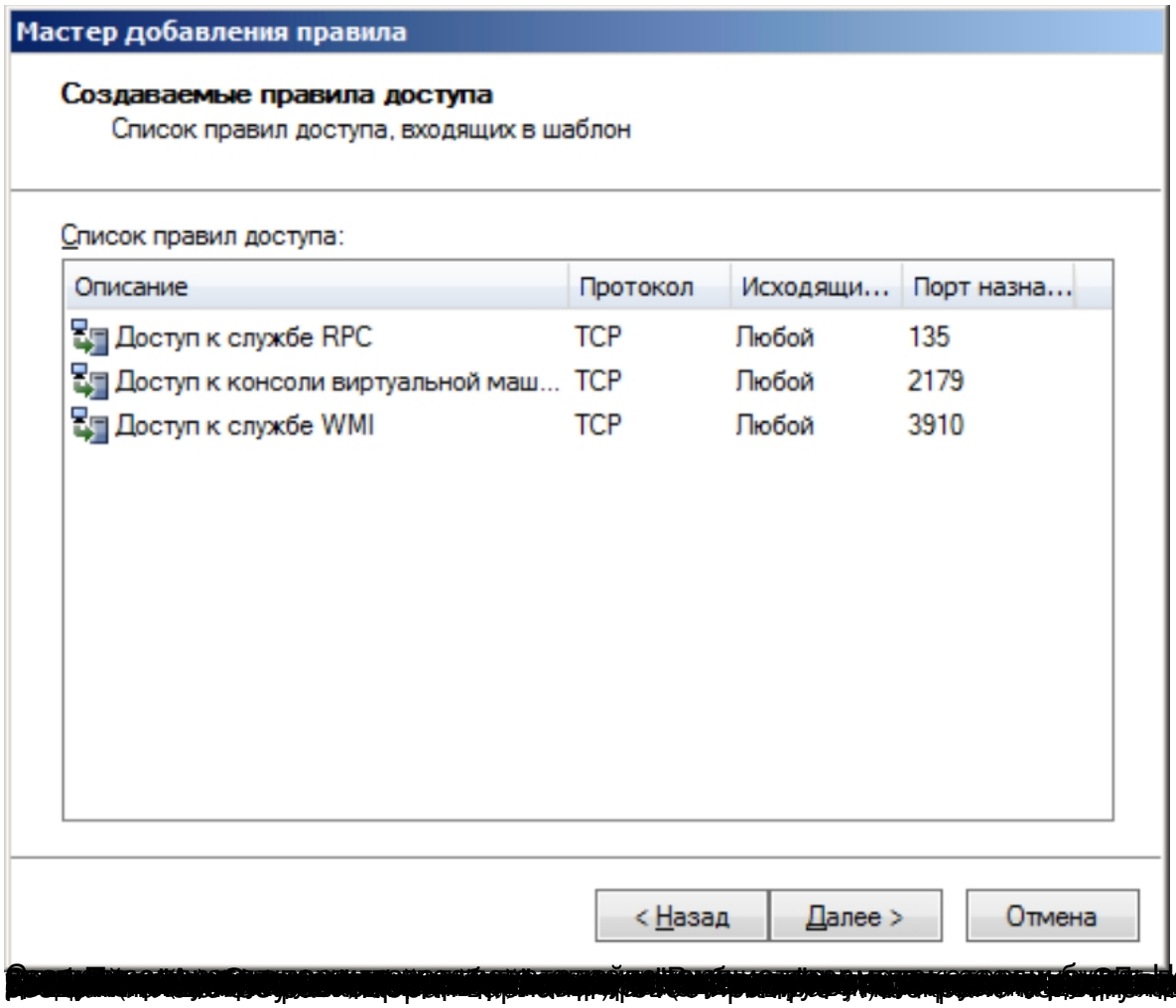
Автор:
27.12.14 20:10 -

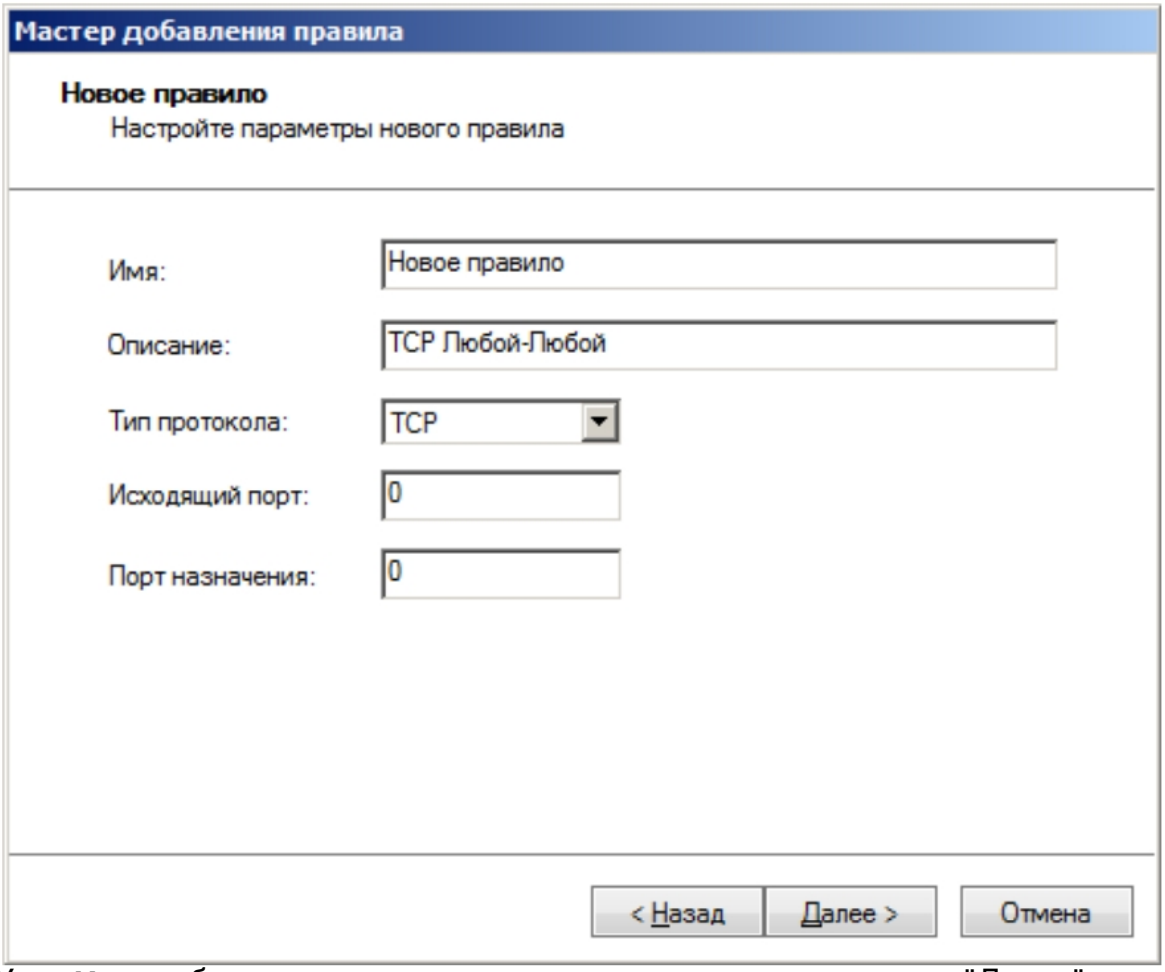


4. Далее на первом диалоге создания правил выбираем вариант "Использовать шаблон", на



Выберите необходимый шаблон и нажмите кнопку "Далее". На экране появится блокирующий диалог


Мастер добавления правила
Создаваемые правила доступа
Список правил доступа, входящих в шаблон
Список правил доступа:
Описание
Протокол
Исходящи...
Порт назна...
Доступ к службе RPC
TCP
Любой
135
Доступ к консоли виртуальной маш...
TCP
Любой
2179
Доступ к службе WMI
TCP
Любой
3910
< Назад
Далее >
Отмена



Укажите необходимые значения параметров и нажмите кнопку "Далее".