

Автор:
27.12.14 20:10 -

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](#)

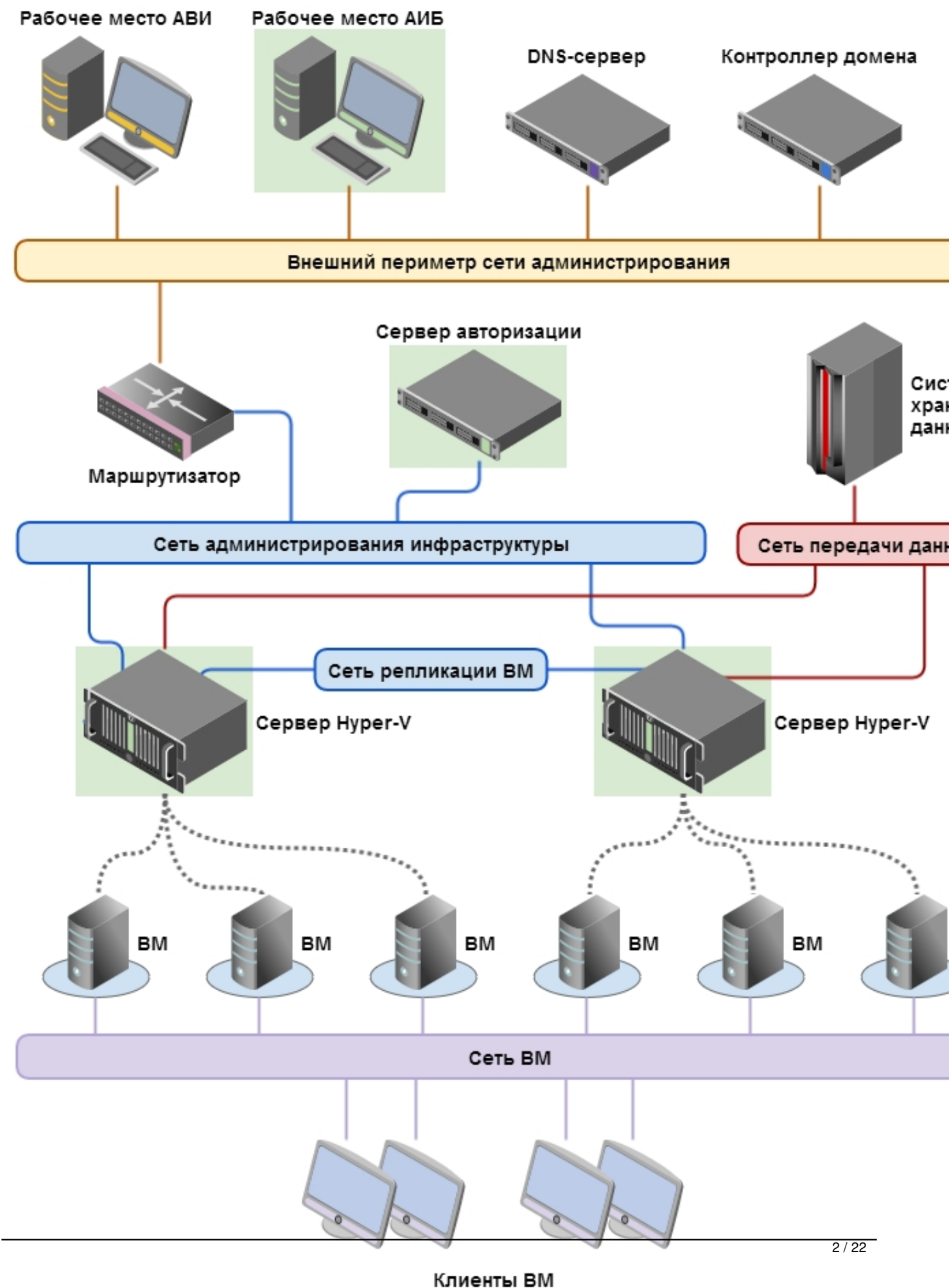
и

[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 -

Администрирование гипервизора Hyper-V












Аудит

Фильтрация событий

Типы событий <input checked="" type="checkbox"/> Успех <input checked="" type="checkbox"/> Уведомление <input checked="" type="checkbox"/> Предупреждение <input checked="" type="checkbox"/> Ошибка	Время событий:	с первого	17/04/2014	5:10:44 PM
		до последнего	17/04/2014	5:10:44 PM
	Компьютер:	*		
	Текст содержит:	*		
			Дополнительно...	Применить

Список событий:

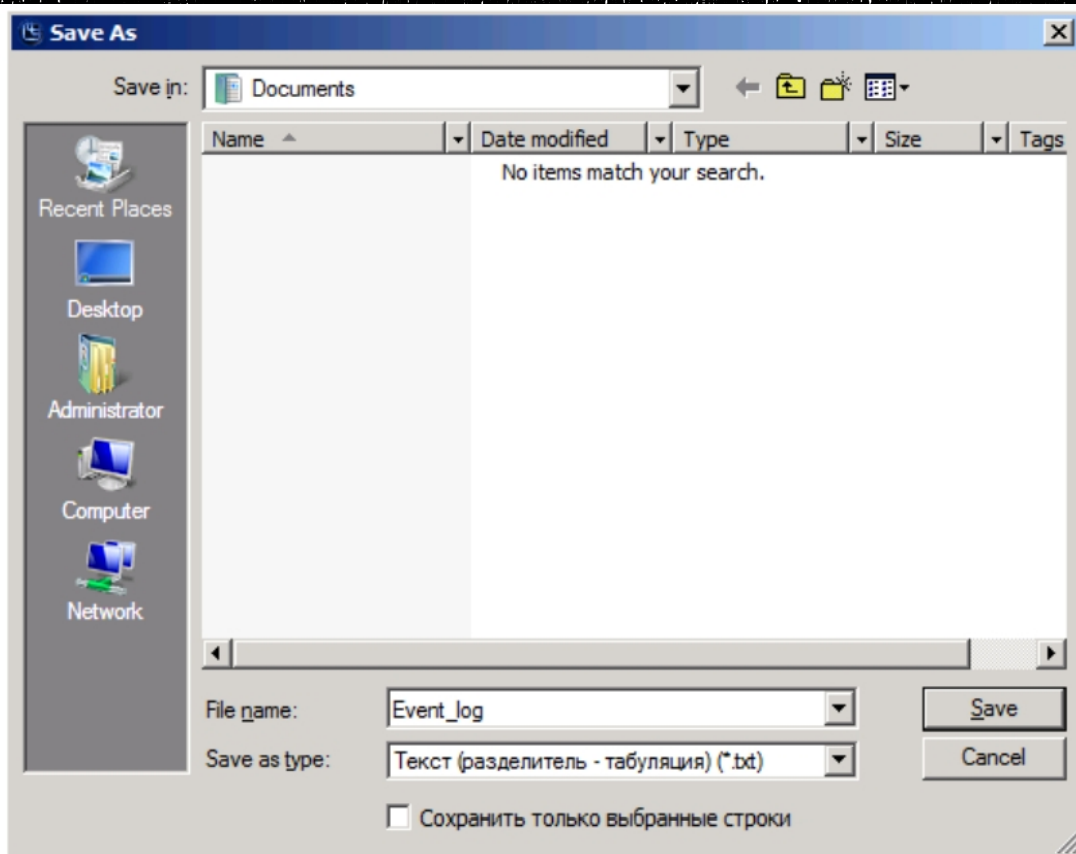
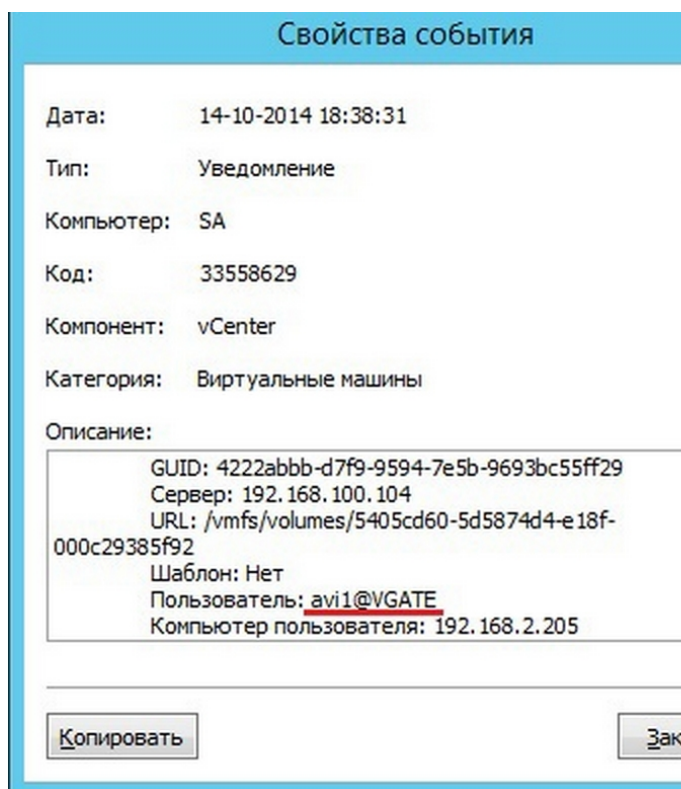
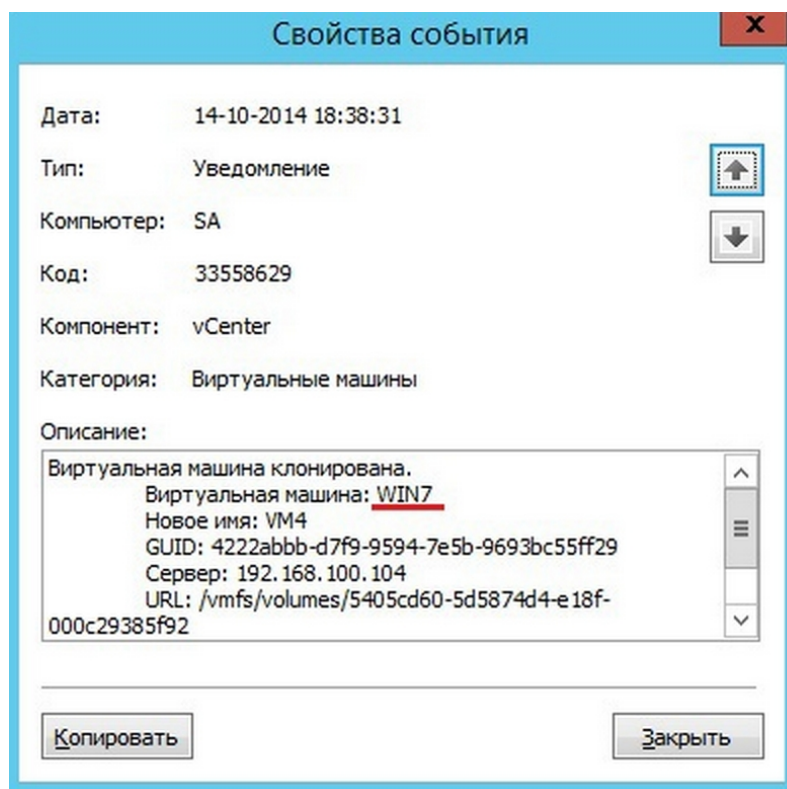
Всего объектов: 2000

Тип	Время	Компьютер	Код события	Компонент	Категория
 Предупреж...	17-04-2014 08:15:50	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
 Успех	17-04-2014 08:15:50	HVAUTHSERVER	16842763	Служба аутентификации	Управление д
 Предупреж...	17-04-2014 08:15:24	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
 Предупреж...	17-04-2014 08:15:03	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
 Успех	17-04-2014 08:15:03	HVAUTHSERVER	16842763	Служба аутентификации	Управление д
 Предупреж...	17-04-2014 08:14:37	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
 Предупреж...	17-04-2014 08:14:16	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
 Успех	17-04-2014 08:14:16	HVAUTHSERVER	16842763	Служба аутентификации	Управление д
 Предупреж...	17-04-2014 08:13:50	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
 Предупреж...	17-04-2014 08:13:29	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
 Успех	17-04-2014 08:13:29	HVAUTHSERVER	16842763	Служба аутентификации	Управление д

Администрирование гипервизора Hyper-V

Автор:

27.12.14 20:10 -



редактировать

Файлы и папки, которые были созданы в папке "Документы" ("Documents") и которые были созданы в папке "Документы" ("Documents")

Автор:
27.12.14 20:10 -

Очистка базы событий

Удалить события ранее:

Настройки генерации событий

Список генерируемых событий:

Строка поиска:

Код события	Состояние	Тип	Категория	Описание события
<input checked="" type="checkbox"/> 134219777	Аудит, SNMP	Ошибка	Целостность	Ошибка службы контроля цел...
<input checked="" type="checkbox"/> 134219782	Аудит	Ошибка	Целостность	Отмена изменений файла %1...
<input checked="" type="checkbox"/> 134219790	Аудит	Ошибка	Целостность	При подсчете контрольной су...
<input checked="" type="checkbox"/> 134219791	Аудит	Ошибка	Целостность	При проверке целостности вир...
<input checked="" type="checkbox"/> 134219792	Аудит	Ошибка	Целостность	При проверке целостности фа...
<input checked="" type="checkbox"/> 134219796	Аудит	Ошибка	Целостность	При подсчете контрольной су...
<input checked="" type="checkbox"/> 134219797	Аудит	Ошибка	Целостность	При проверке целостности гос...
<input checked="" type="checkbox"/> 134234113	Аудит, SNMP	Ошибка	Служба	Не удалось запустить службу ...
<input checked="" type="checkbox"/> 134234115	Аудит, SNMP	Ошибка	Служба	Не удалось остановить служб...
<input checked="" type="checkbox"/> 134234121	Аудит, SNMP	Ошибка	Служба	Не удалось запустить службу ...
<input checked="" type="checkbox"/> 134234123	Аудит, SNMP	Ошибка	Служба	Не удалось остановить служб...
<input checked="" type="checkbox"/> 134250499	Аудит	Ошибка	Развертывание	При установке агента vGate н...
<input checked="" type="checkbox"/> 134250500	Аудит	Ошибка	Развертывание	При удалении агента vGate с с...
<input checked="" type="checkbox"/> 134283266	Аудит	Ошибка	Управление доступом	Переименование защищаемого...
<input checked="" type="checkbox"/> 134283267	Аудит	Ошибка	Управление доступом	Создание защищаемого объек...

Включено: 426, выключено: 0.

Автор:
27.12.14 20:10 -

Защищаемые серверы

Список защищаемых серверов:

Всего объектов: 0

Имя	Тип	Версия	С...	Уровень	Катег...	Разре...	Поясн...

- + Сервер виртуализации
- + Автономный сервер
- ✕ Удалить
- ✎ Редактировать
- Назначить метку
- Экспорт

Обновить

Настройка нового сервера "Hyper-V виртуализация". На экране появится мастер

Мастер добавления нового сервера Hyper-V в список защищаемых серверов

Настройки соединения с сервером Hyper-V
Укажите полное доменное имя или IP-адрес сервера виртуальной инфраструктуры, имя (в формате 'domain\account') и пароль пользователя, обладающего правами администратора на этом сервере

Сервер будет добавлен в список защищаемых серверов. Агент vGate будет установлен автоматически

Сервер:

Пользователь:

Пароль:

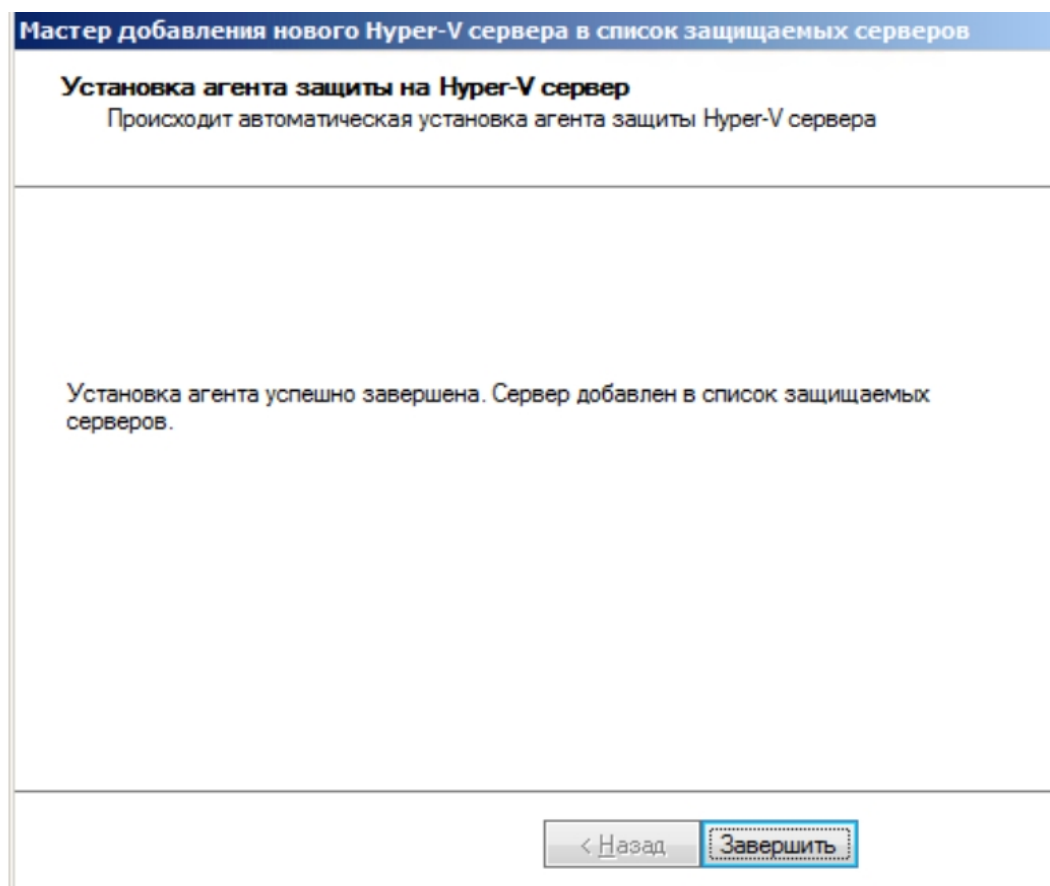
☐ Сохранить имя пользователя и пароль
Эти настройки будут использованы при добавлении следующих серверов

< Назад Далее > Отмена

Настройка нового сервера "Hyper-V виртуализация". На экране появится мастер

Автор:

27.12.14 20:10 -



Вывод информации об установленных агентах защиты Hyper-V серверов

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

- + Переустановить
- × Удалить
- || Приостановить контроль

Вывод информации об установленных агентах защиты Hyper-V серверов

Развертывание

Список защищаемых серверов

Всего объектов: 2

Имя	Статус агента	Версия агента	Сокеты
192.168.2.20	Установка		1
192.168.2.21	Запущен	1.0.251.0	1

- + Установить
- × Удалить
- ▶ Возобновить контроль

При установке агента защиты Hyper-V параметр "Статус"



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 -

Новый пользователь

Пользователь:

Пароль:

Подтверждение:

Полномочия учетной записи:

- ☐ Администратор информационной безопасности
- ☐ Оператор учетных записей
- ☐ Срок действия пароля неограничен
- ☐ Учетная запись отключена
- ☒ Сменить пароль при следующем входе в систему
- ☒ Разрешено скачивать файлы виртуальных машин

ОК Отмена

Убедившись в корректности введенных параметров, нажмите кнопку "ОК".

Автор:

27.12.14 20:10 -

Политики паролей пользователей

Максимальный срок действия пароля: 30 дней

Минимальная длина пароля: 1 символов

Хранить историю: 4 паролей

Разница при смене пароля: 4 символов

Минимальное количество классов символов: 1

Отключить учетную запись, неиспользуемую более: 90 дней

Отключить учетную запись после: 3 неуспешных попыток входа


ОК Отмена

В настройках безопасности системы можно задать следующие параметры:

Автор:

27.12.14 20:10 -

Консоль управления vGate for Hyper-V



vGate for Hyper-V

Защищаемые серверы

Развертывание

Виртуальные машины

Конфигурация

Политики безопасности

Метки безопасности






Учетные записи

О продукте



Аудит


Метки безопасности


Категории конфиденциальности: Всего объектов: 5


Имя	Описание	Наборы политик безопасности
 Желтый		
 Зеленый		
 Красный		
 Оранжевый		
 Синий		


Уровни конфиденциальности: Всего объектов: 2


Имя	Описание	Наборы политик безопасности
 Неконфиденциально		
 Для служебного пользования		


 Настроить матрицу сочетаний уровней и категорий конфиденциальности


 Добавить


 Удалить


 Редактировать


 Назначить политику


 Отменить назначение

 Обновить

 Редактировать

 Назначить политику

 Отменить назначение

 Обновить

Автор:

27.12.14 20:10 -

Метка безопасности

Категории конфиденциальности:

Категория	Описание
<input type="checkbox"/> Желтый	
<input type="checkbox"/> Зеленый	Описание
<input type="checkbox"/> Красный	
<input type="checkbox"/> Оранжевый	
<input type="checkbox"/> Синий	

Уровень конфиденциальности:

Уровень

☐ Неконфиденциально

☒ Для служебного пользования

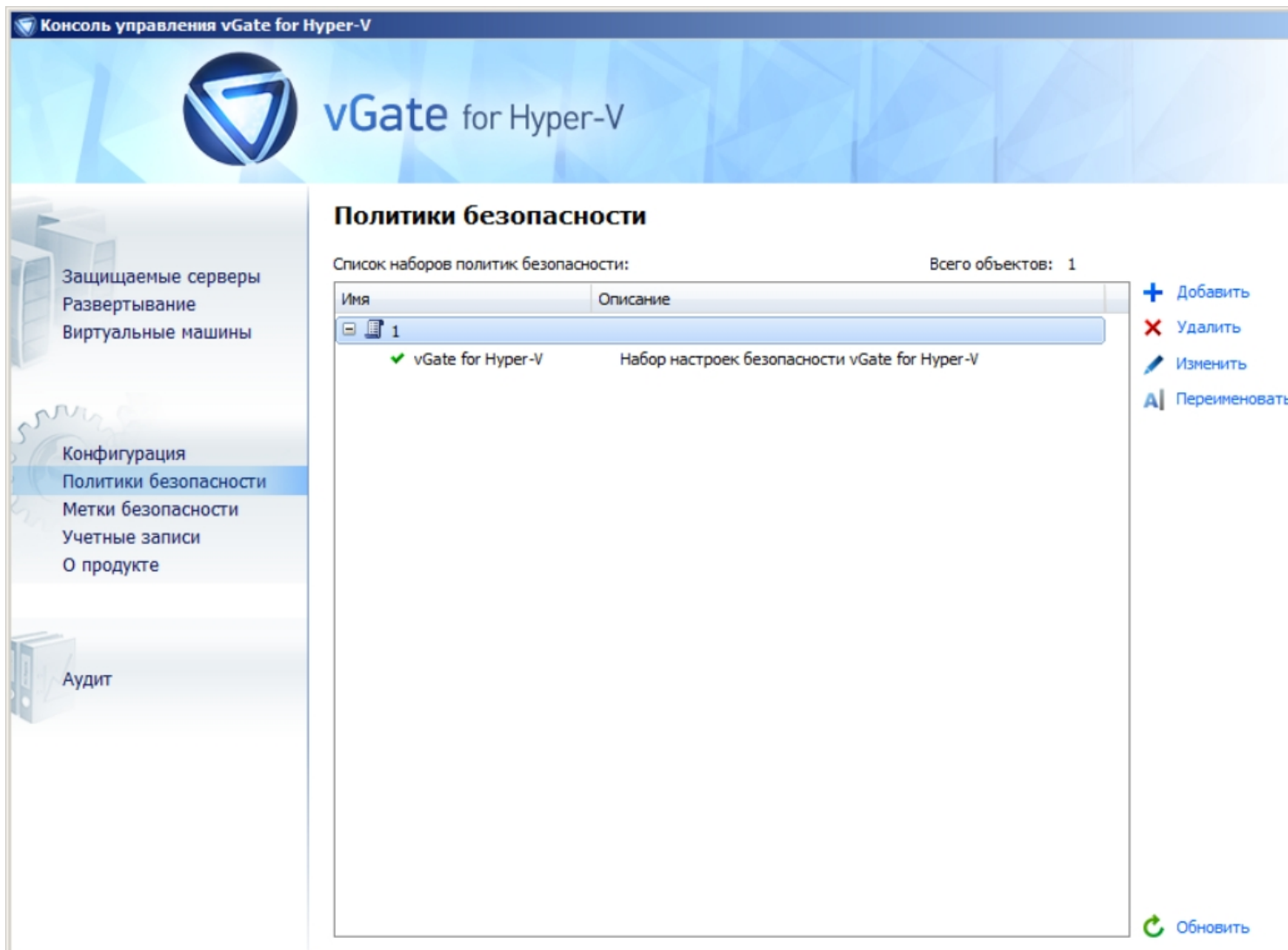
☒ Разрешено исполнять ВМ с меньшим уровнем

OK Отмена

Внимание! При выборе категории конфиденциальности и уровня конфиденциальности необходимо учитывать, что для выполнения виртуальной машины с меньшей категорией конфиденциальности необходимо, чтобы виртуальная машина с большей категорией конфиденциальности была настроена на выполнение. В противном случае виртуальная машина не будет запущена.

Автор:

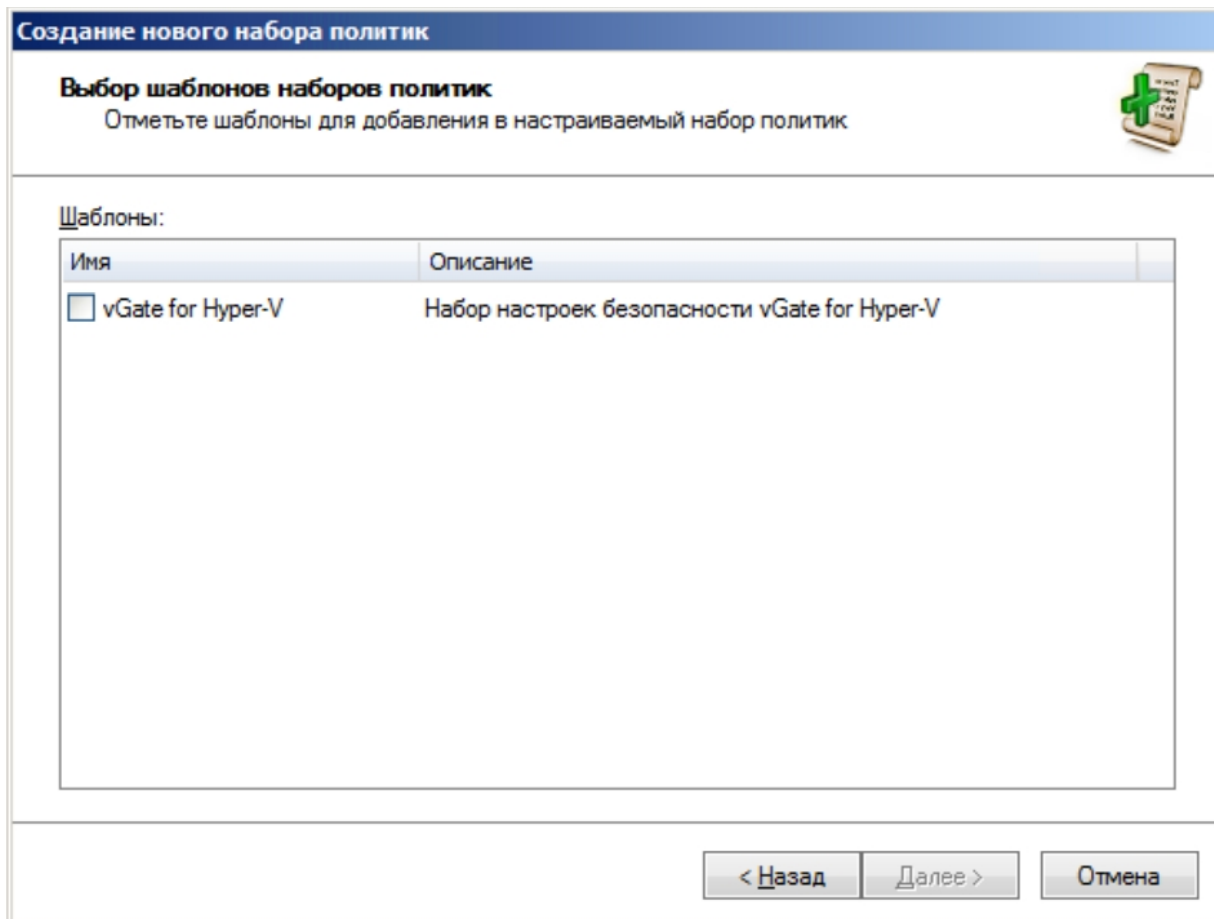
27.12.14 20:10 -



Далее нажмите кнопку "Добавить" и создайте новый шаблон политик на базе

Автор:

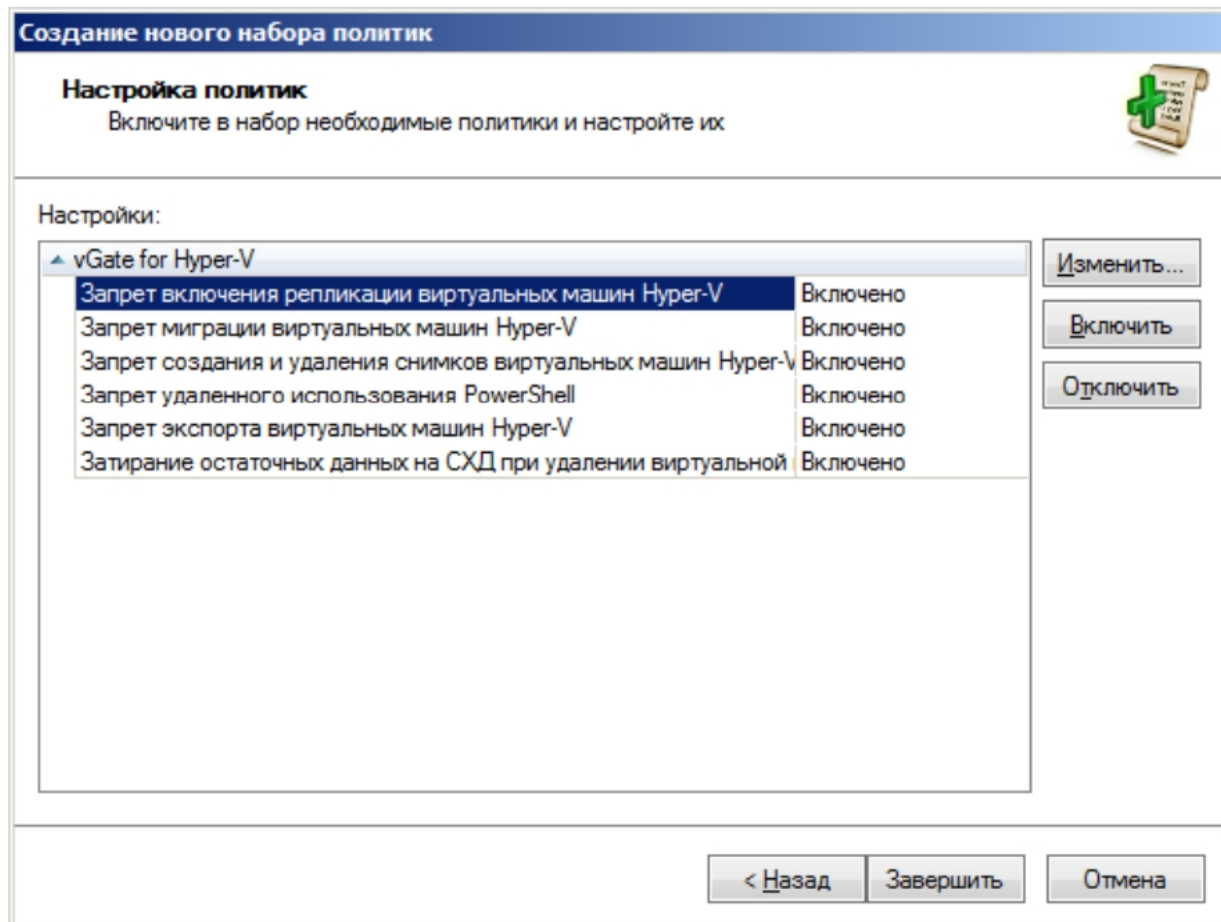
27.12.14 20:10 -



На экране появится диалог настройки политик:

Автор:

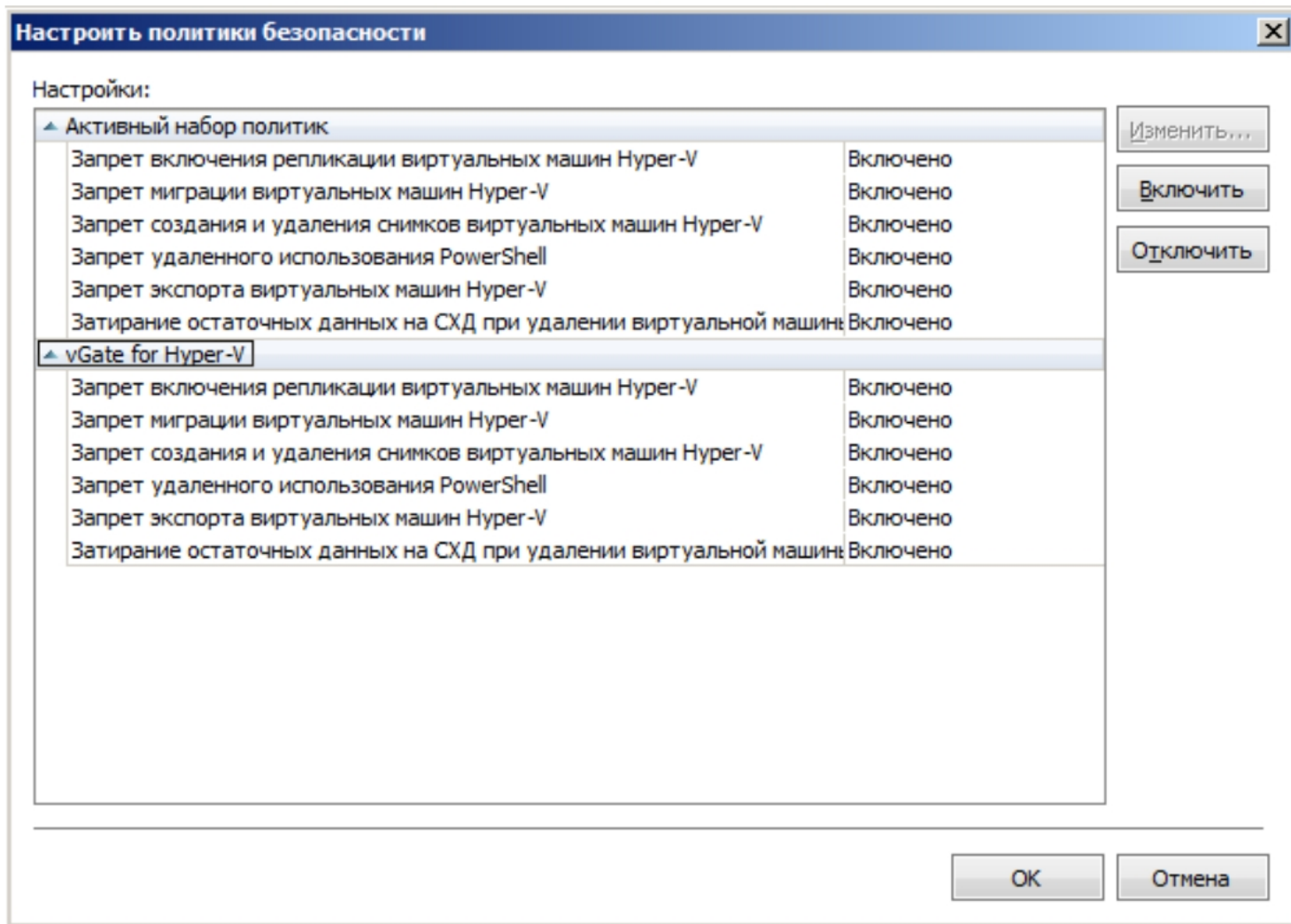
27.12.14 20:10 -



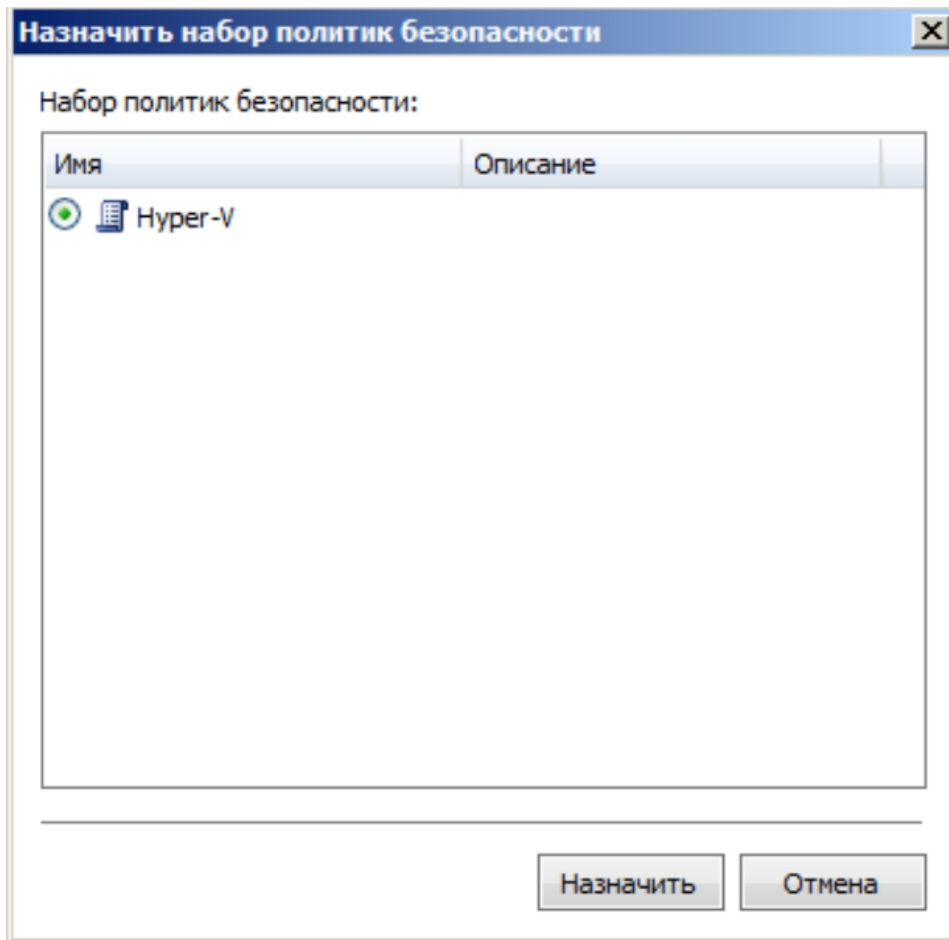
Внимание! При изменении параметров политики, необходимо перезагрузить виртуальную машину.

Автор:

27.12.14 20:10 -



Автор:
27.12.14 20:10 -



Назначение политик безопасности для виртуальной машины Hyper-V

Автор:
27.12.14 20:10 -

Защищаемые серверы

Список защищаемых серверов:

Всего объектов: 3

Имя	Тип	Версия	С...	Уровень	Катег...	Разре...	Поясн...
192.168.2.10	Автоно...						Сервер...
192.168.2.20	Сервер...	Windows Server 2...	1	Неконф...		Да	hvVmS...
192.168.2.21	Сервер...	Windows Server 2...	1	Неконф...		Да	hvVmS...

Сервер виртуализации

Автономный сервер

Удалить

Редактировать

Назначить метки

Экспорт

Обновить

Правила доступа для 192.168.2.10:

Всего правил: 5

Описание	Состо...	Пользоват...	Компьютер...	Прото...	Исход...	Порт н...
Доступ к вспомогатель...	Вкл	admin@VGATE	*	TCP	Любой	3908
Доступ к отчетам для ...	Вкл	admin@VGATE	*	TCP	Любой	5432
Доступ к службе управ...	Вкл	admin@VGATE	*	TCP	Любой	3802
Доступ к службе управ...	Вкл	admin@VGATE	*	TCP	Любой	3906
Статус операций по уп...	Вкл	admin@VGATE	*	TCP	Любой	3803

Создать правило

Удалить

Свойства

Выключить

Экспорт

Обновить

Правила доступа для 192.168.2.20:

Всего правил: 3

Описание	Состо...	Пользоват...	Компьютер...	Прото...	Исход...	Порт н...
Доступ к консоли вирт...	Вкл	avi@VGATE	*	TCP	Любой	2179
Доступ к службе RPC	Вкл	avi@VGATE	*	TCP	Любой	135
Доступ к службе WMI	Вкл	avi@VGATE	*	TCP	Любой	3910

Создать правило

Удалить

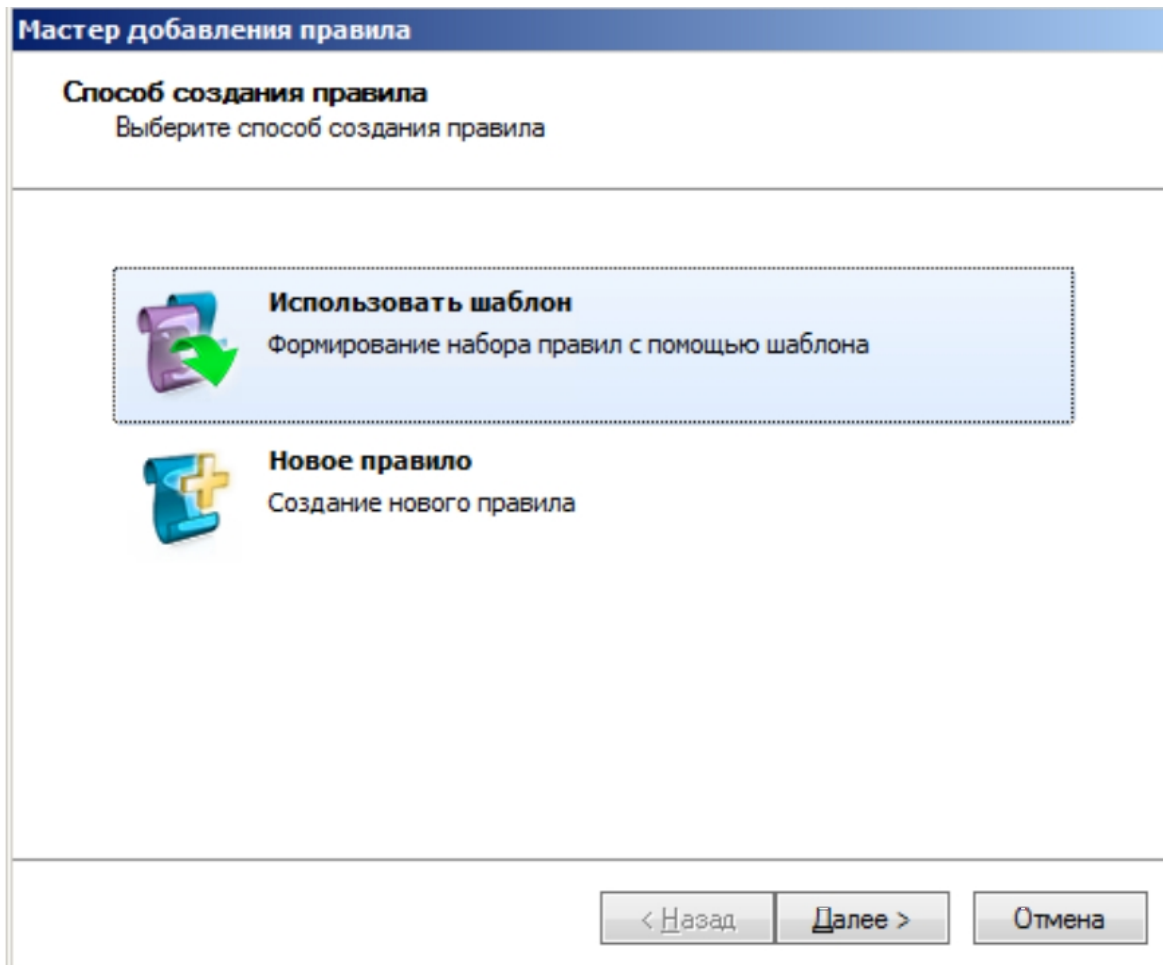
Свойства

Выключить

Экспорт

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

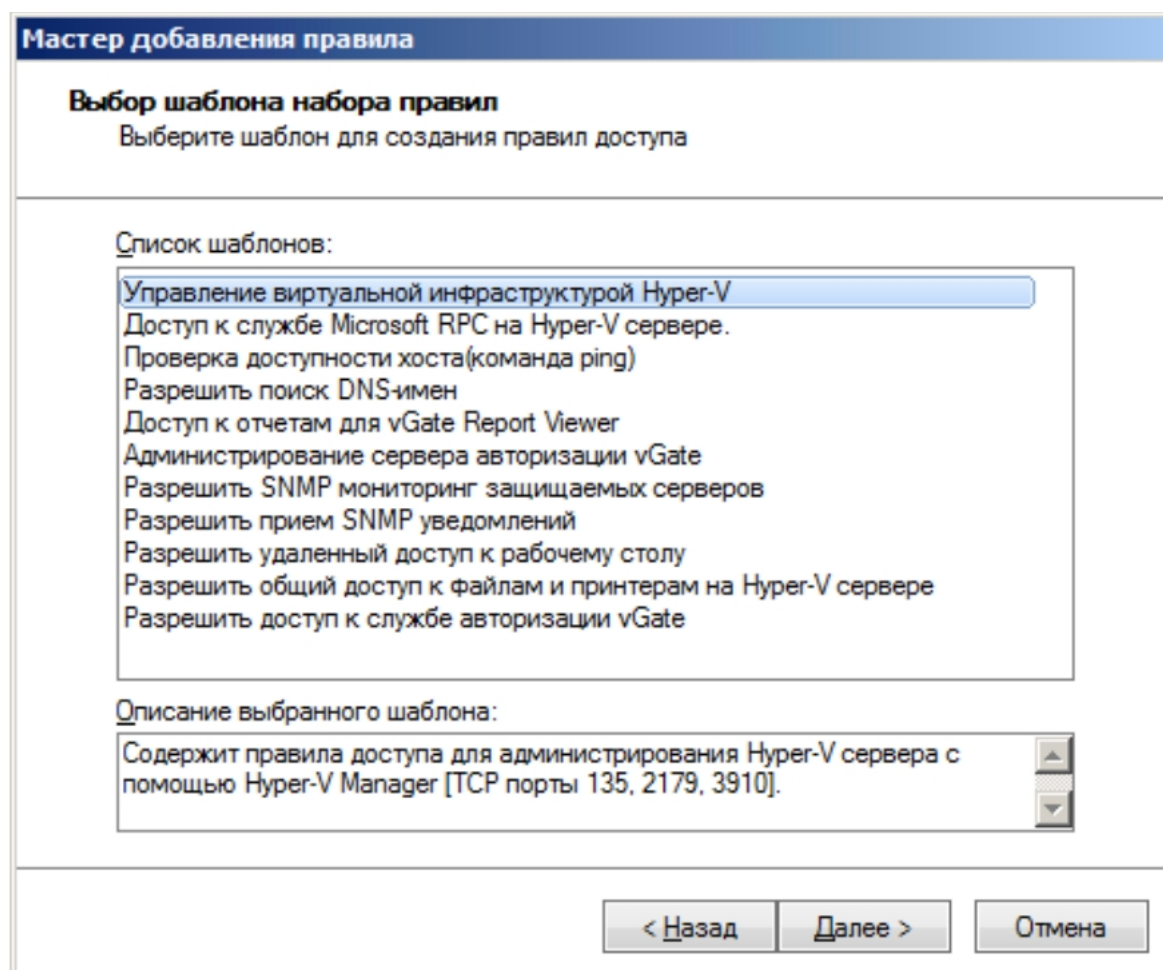
Автор:
27.12.14 20:10 -



экрана на предыдущем шаге создания правил был выбран вариант "Использовать шаблон", на

Автор:

27.12.14 20:10 -



Мастер добавления правила

Выбор шаблона набора правил
Выберите шаблон для создания правил доступа

Список шаблонов:

- Управление виртуальной инфраструктурой Hyper-V
- Доступ к службе Microsoft RPC на Hyper-V сервере.
- Проверка доступности хоста(команда ping)
- Разрешить поиск DNS-имен
- Доступ к отчетам для vGate Report Viewer
- Администрирование сервера авторизации vGate
- Разрешить SNMP мониторинг защищаемых серверов
- Разрешить прием SNMP уведомлений
- Разрешить удаленный доступ к рабочему столу
- Разрешить общий доступ к файлам и принтерам на Hyper-V сервере
- Разрешить доступ к службе авторизации vGate

Описание выбранного шаблона:

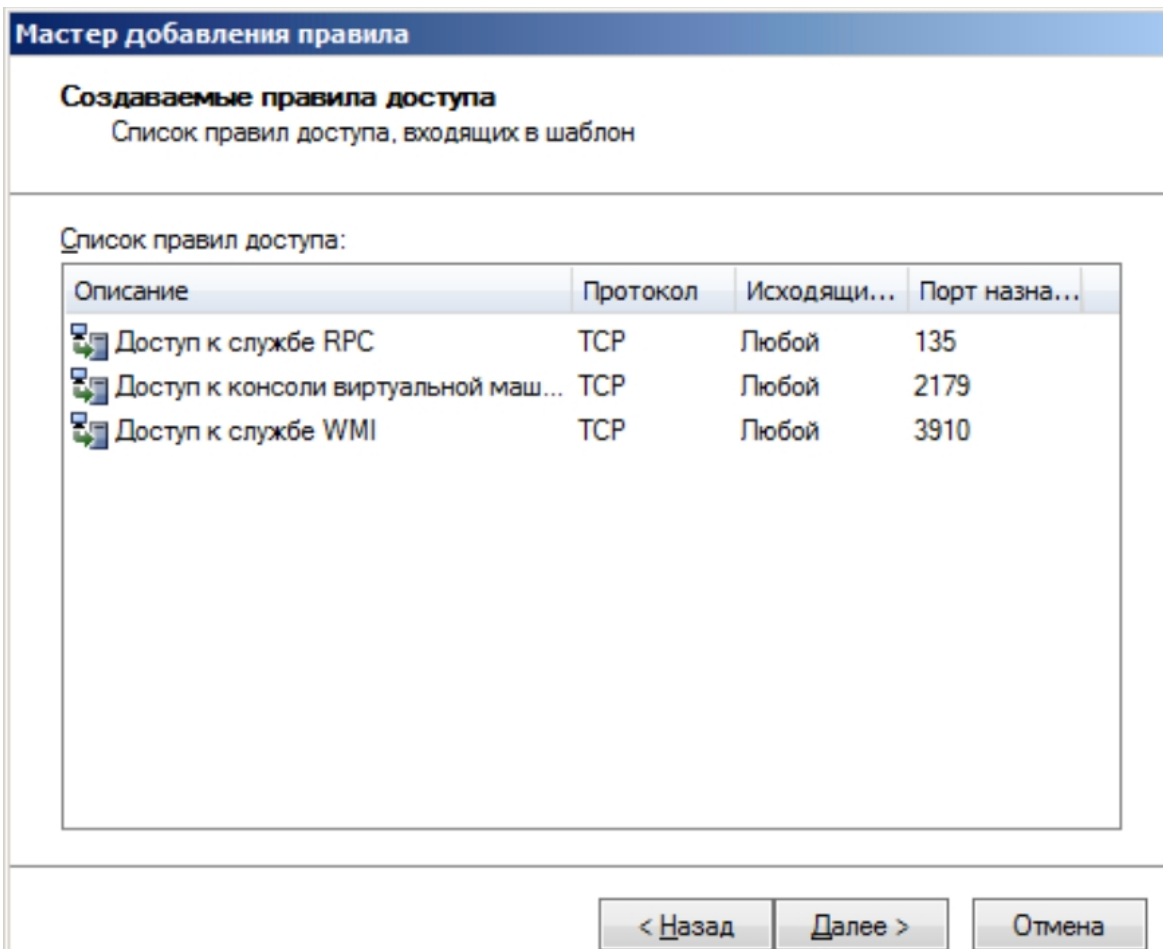
Содержит правила доступа для администрирования Hyper-V сервера с помощью Hyper-V Manager [TCP порты 135, 2179, 3910].

< Назад Далее > Отмена

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

Автор:

27.12.14 20:10 -



Указано, що найбільш значущими параметрами на жито є класи "Далеко" і "Трохи", тільки в