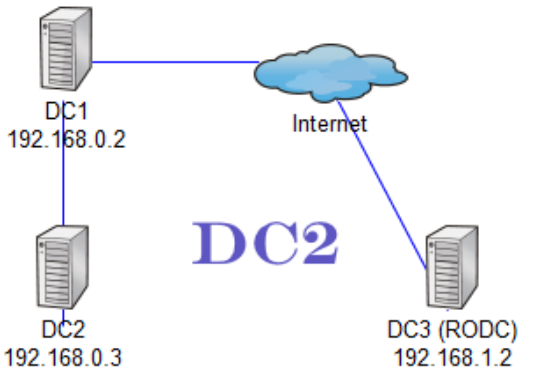
« **Установка контроллера домена только для чтения (RODC) на базе Windows 2012 R2 (core)**

**Первый контроллер домена в лесу, на базе Windows 2012 R2. Настройка служб AD DS, DNS, DHCP** »

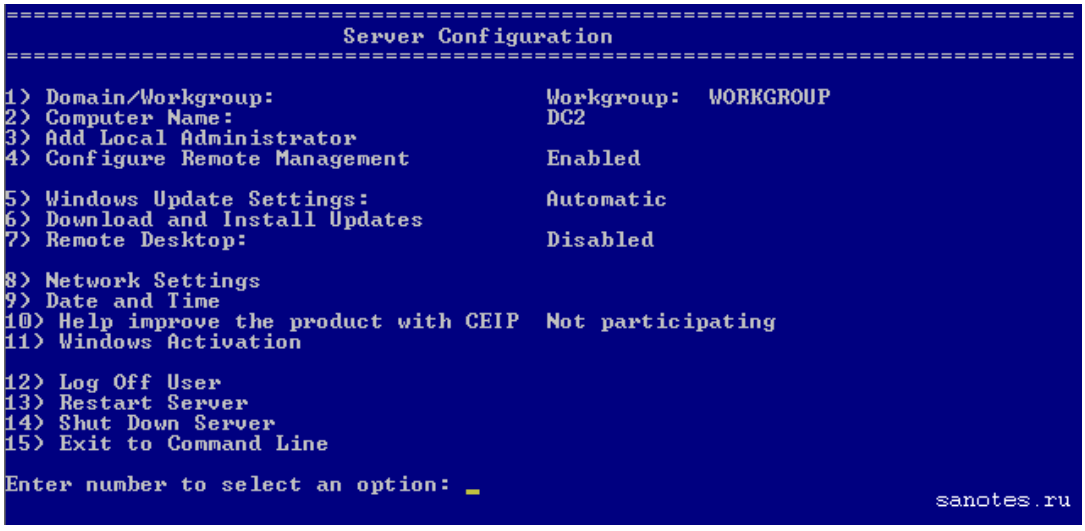
# Установка дополнительного контроллера домена на базе Windows 2012 R2 (core)


**Шаг 3: Установка второго контроллера домена. Настройка служб AD DS, DNS, DHCP.**

В предыдущей **заметке**, мы развернули первый контроллер домена на предприятии а так же настроили службу DNS, DHCP. Второй и **последующий** контроллеры будут у нас без GUI в core-варианте.

Предварительно настроим сервер при помощи **sconfig**, назначим имя: dc2, настроим сеть, установим последние обновления, включим удаленное управление.




Затем добавим роль AD DS. Рассмотрим два варианта развертывания служб AD DS на сервере с Windows core.

Первый вариант это добавить наш сервер в Server Manager первого сервера, и поднять роль при помощи графического интерфейса как мы делали это в самом **начале**. Для этого необходимо выполнить ряд условий:

1) На сервере с Windows Core активировать удаленное управление. Например при помощи 4-го пункта меню в sconfig (Configure Remote Management) или аналогично выполнив следующие команды в консоле:

```
WinRM quickconfig
```

и нажать yes. В powershell:

```
Configure-SMRemoting.exe -enable
```

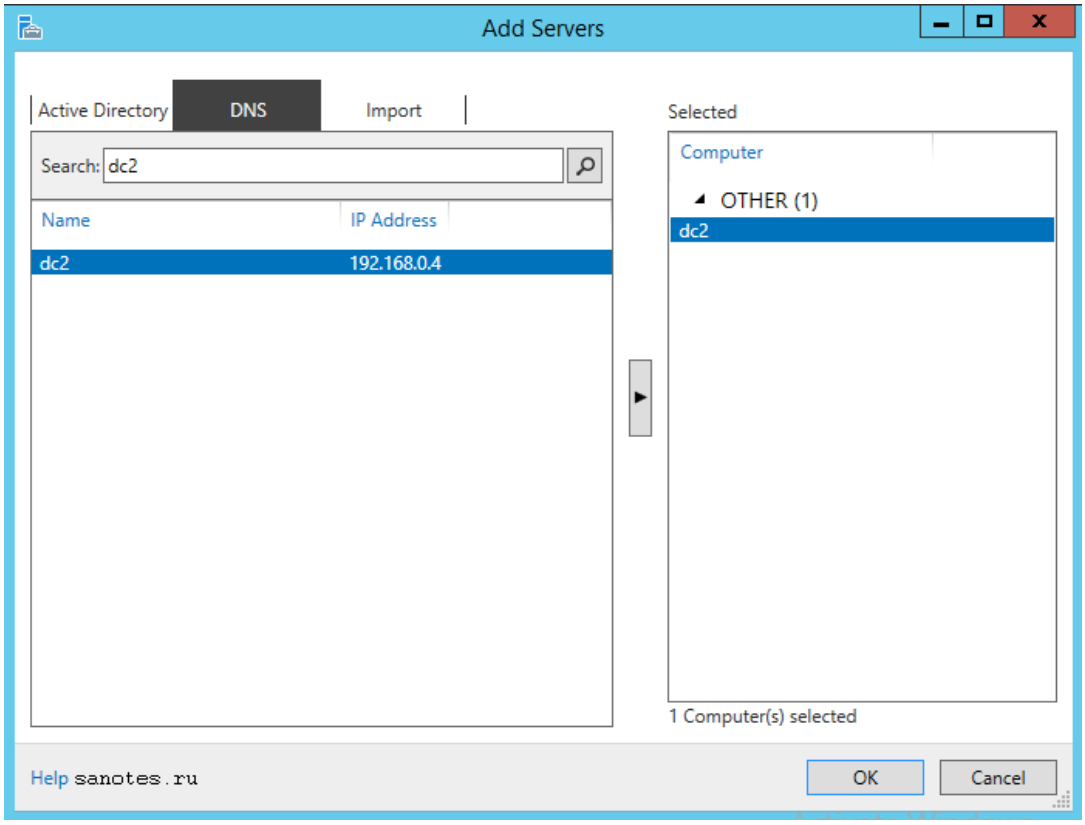
2) Разрешить ряд правил на файрволе для обнаружения сервера по dns:

```
Enable-NetFirewallRule -DisplayGroup "File and Printer Sharing"
```

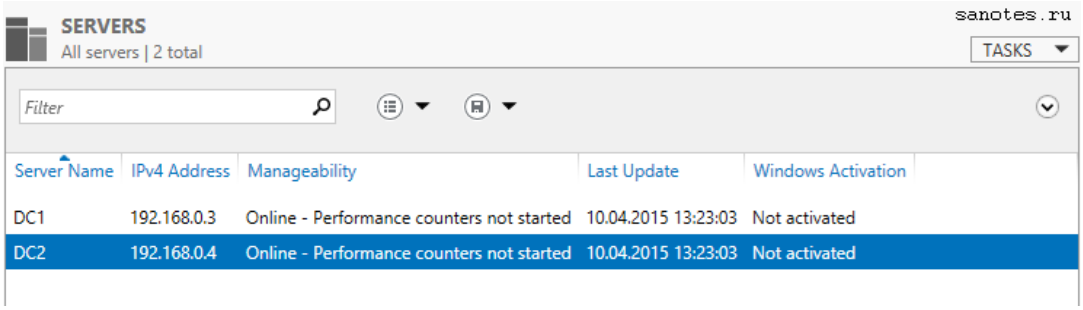
3) Добавить сервер в домен. Во время выполнения команды, потребуются ввести учетные данные доменного админа. Перезагрузить сервер.

```
Add-Computer -DomainName test.ru
```

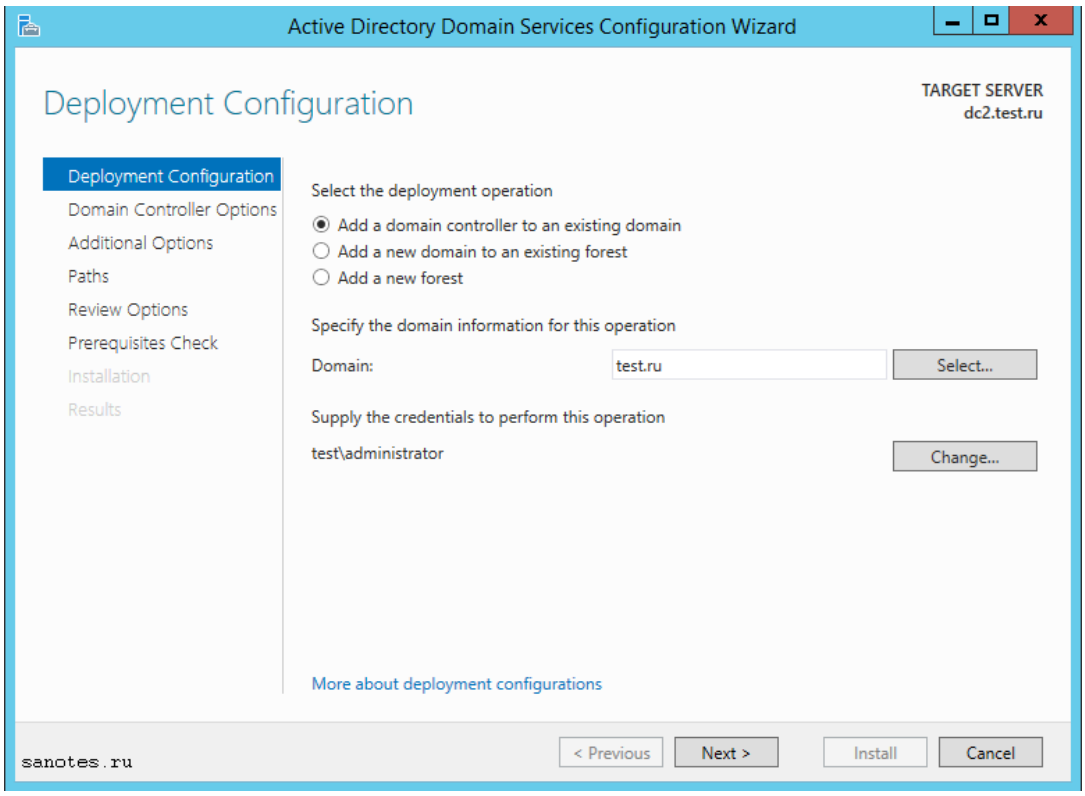
4) На управляющем сервере в Server Manager нажать Manage и выбрать Add Servers. В появившемся окне Add Servers перейти на вкладку DNS и найти там наш сервер. Нажать OK.



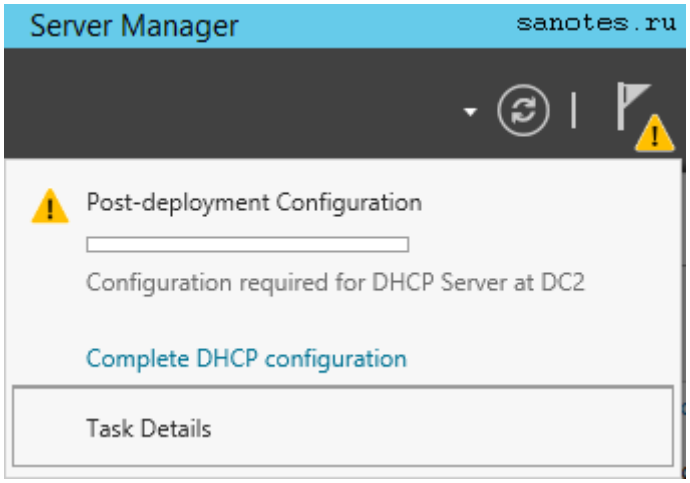

Если видим, что в поле Manageability запись изменилась на 'Online — Performance counters not started' то все в порядке и можно приступать к процессу развертывания служб AD DS при помощи мастера добавления ролей и компонентов.




После чего можно будет стандартным образом отметь роли для установки и сконфигурировать роль AD DS. Необходимо только выбрать, что домен будет вторым в существующем домене (Add a domain controller to an existing domain). И затем нажимая кнопку далее дойти до завершающего этапа установки.




После перезагрузки, снова зайдем в диспетчер сервера, запустим пиктограмму треугольника с восклицательным знаком и завершим конфигурацию DHCP-сервера выбором **Complete DHCP Configuration.**




Второй способ развертывания служб AD на сервере с windows core, традиционно выполняется при помощи 'dcpromo', но на мой взгляд удобнее и быстрее для этих целей использовать команды powershell. К тому же с началом выхода 2012 сервера, инструмент 'dcpromo' считается устаревшим и не рекомендуемым к использованию. Например, в полном варианте 2012/2012R2 сервера 'dcpromo' уже не работает, предлагая воспользоваться диспетчером сервера, хотя в core-варианте возможность запуска до сих пор присутствует. Итак приступим к установке:

Сначала добавим роль служб и компонентов Active Directory, DNS и заодно DHCP:

```
Install-windowsfeature -name AD-Domain-Services,DNS,DHCP -IncludeManagementT
```

либо вариант команды с использованием xml-скрипта, который мы могли сохранить ранее на этапе добавления ролей и компонентов в графическом варианте:

```
Install-windowsfeature -ConfigurationFilePath C:\DeploymentConfigTemplate.xm
```

Импорт модулей и команд AD выполним при помощи команды:

```
Import-Module ADDSDeployment
```

Теперь что бы повысить роль сервера до контроллера домена набираем:

```
Install-ADDSDomainController -DomainName "test.ru" -Credential (get-credenti
```

где,

Install-ADDSDomainController — установить дополнительный контроллер домена,
DomainName «test.ru» — имя домена,
Credential (get-credential) — учетные данные для авторизации в домене, можно задать комбинацию домен\логин как в примере выше.

После, скрипт запросит пароль администратора домена, указанный в параметре Credential. Затем, необходимо будет указать пароль для режима восстановления (Directory Services Restore Mode — DSRM) — SafeModeAdministratorPassword, либо указать его как параметр выше в команде. Нажимаем Yes и дожидаемся окончания процесса установки, после чего сервер будет перезагружен. На выходе получим дополнительный (Replica) контроллер в домене test.ru.

Ту же самую операцию можно выполнить при помощи powershell скрипта, который можно подсмотреть на этапе установки Review Options мастера развертывания Active Directory Domain Services Configuration Wizard, если нажать кнопку Review Script.

Для установки второго контроллера домена в существующем домене содержимое скрипта будет следующим:

```
Import-Module ADDSDeployment
Install-ADDSDomainController `
-NoGlobalCatalog:$false `
-CreateDnsDelegation:$false `
-Credential (Get-Credential) `
-CriticalReplicationOnly:$false `
-DatabasePath "C:\Windows\NTDS" `
-DomainName "test.ru" `
-InstallDns:$true `
-LogPath "C:\Windows\NTDS" `
-NoRebootOnCompletion:$false `
-ReplicationSourceDC "DC1.test.ru" `
-SiteName "Default-First-Site-Name" `
-SysvolPath "C:\Windows\SYSVOL" `
-Force:$true
```

Текстовый файл необходимо сохранить с расширением .ps1 и в консоли powershell выполнить:

```
./script_name.ps1
```

Потребуется указать пароль администратора домена и пароль для режима восстановления каталогов (DSRM).

Подробнее о возможных параметрах командлета Install-ADDSDomainController читаем **здесь**.

Что бы перечислить все возможные командлеты по настройке ролей Active Directory набираем:

```
Get-command -module ADDSDeployment
```

В результате отобразится следующий список:

Add-ADDSReadOnlyDomainControllerAccount — Создание учетной записи контроллера домена только для чтения.

Install-ADDSDomain — Установить первый контроллер домена в дочернем или дереве домена.

Install-ADDSDomainController — Установить дополнительный контроллер домена.

Install-ADDSForest — Установить первый контроллер в новом лесу.

Test-ADDSDomainControllerInstallation — Проверка предварительных требований для установки контроллера домена в Active Directory.

Test-ADDSDomainControllerUninstallation — Проверка удаления сервиса AD с сервера.

Test-ADDSDomainInstallation — Проверка предварительных требований для установки нового домена в Active Directory.

Test-ADDSForestInstallation — Проверка предварительных требований для установки нового леса Active Directory.

Test-ADDSReadOnlyDomainControllerAccountCreation — Проверка предварительных требований для добавления учетной записи контроллера домена только для чтения (RODC).

Uninstall-ADDSDomainController — Удаление контроллера домена с сервера.

После перезагрузки завершим конфигурацию DHCP-сервера при помощи команд:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Microsoft\ServerManager\Roles\12 -Name
```

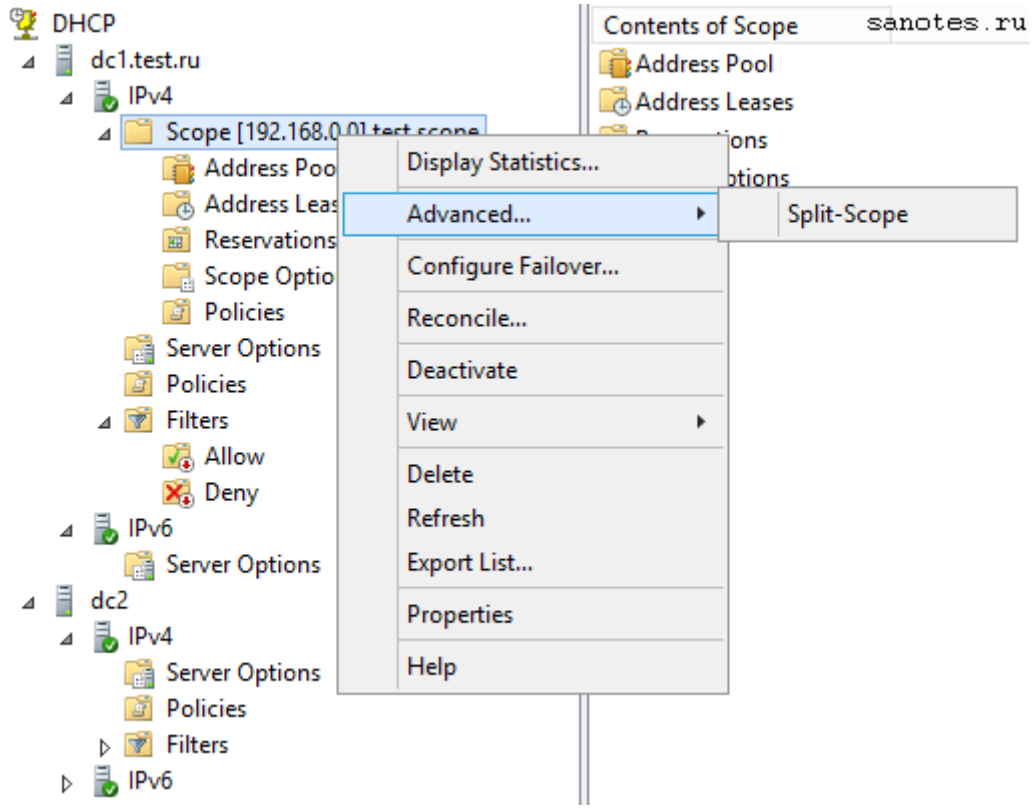
```
Restart-Service DHCPServer
```

**Шаг4: Установка второго контроллера домена. Настройка резервирования службы DHCP.**

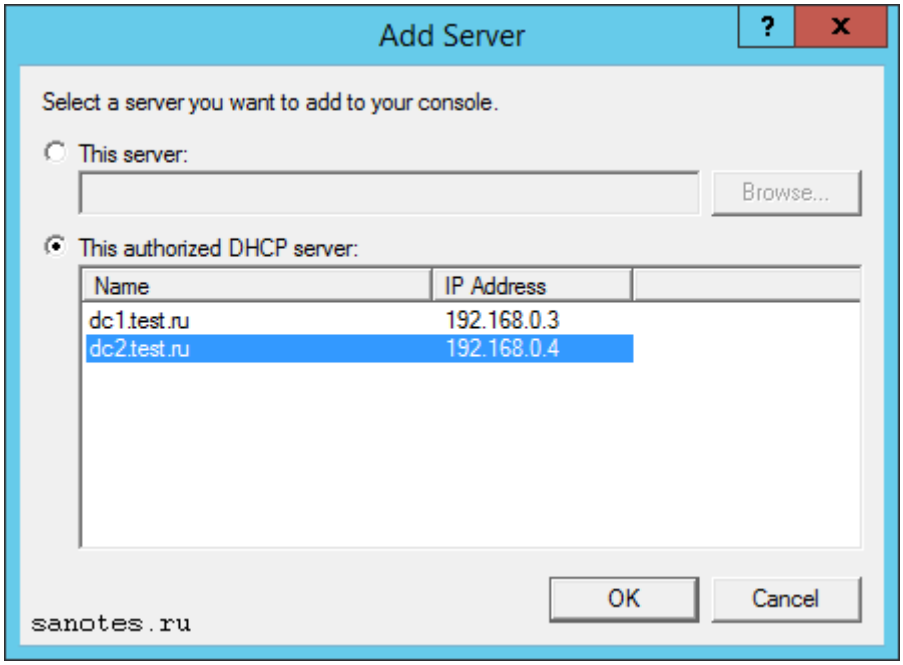
Поскольку в нашей сети уже есть один авторизованный DHCP-сервер с настроенной областью, то теперь необходимо решить как будет работать служба DHCP на дополнительном контроллере server core. Возможны два варианта:

**1) Использование распределенных областей (Split Scope)** — Распределение адресного пространства между двумя серверами. Например одному серверу назначаются 70 или 80% адресов области, а оставшиеся 20 или 30% — дополнительному серверу. Если клиентам не удается получить IP-адрес от основного сервера, то они могут получить его у дополнительного сервера.

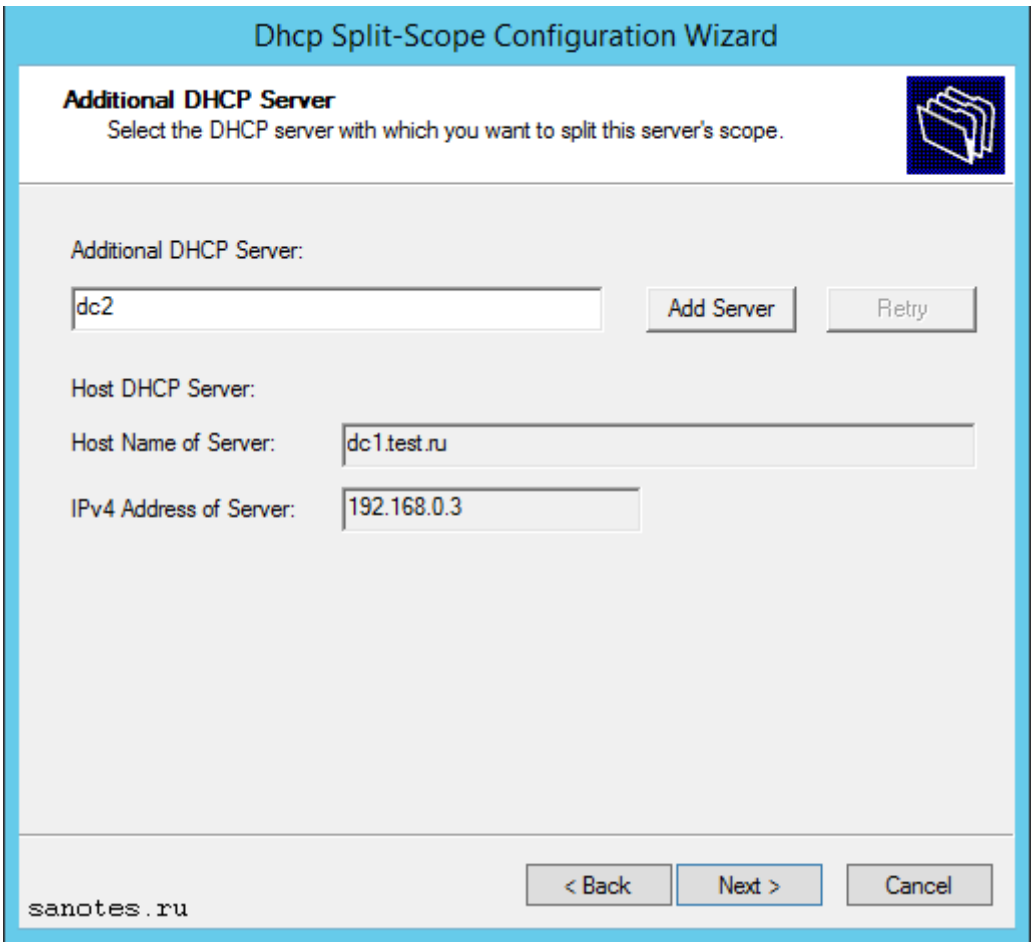
Для создания разделенной области, на основном сервере, открываем оснастку DHCP, щелкаем правой кнопкой по имени области и выбираем **Advanced -> Split-Scope.**



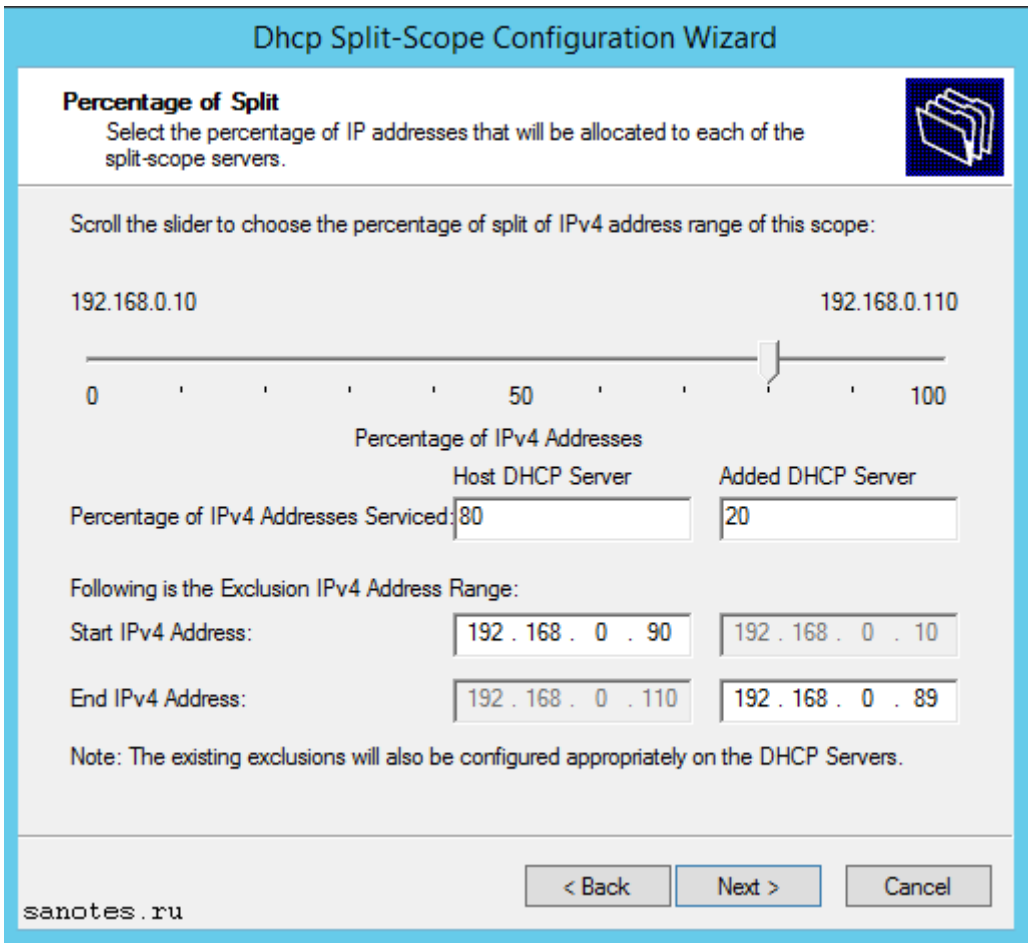

Нажимаем Далее, затем добавляем сервер нажатием **Add Server** и в поле **This authorized DHCP server** выбираем второй сервер.




Жмем ОК и Далее.

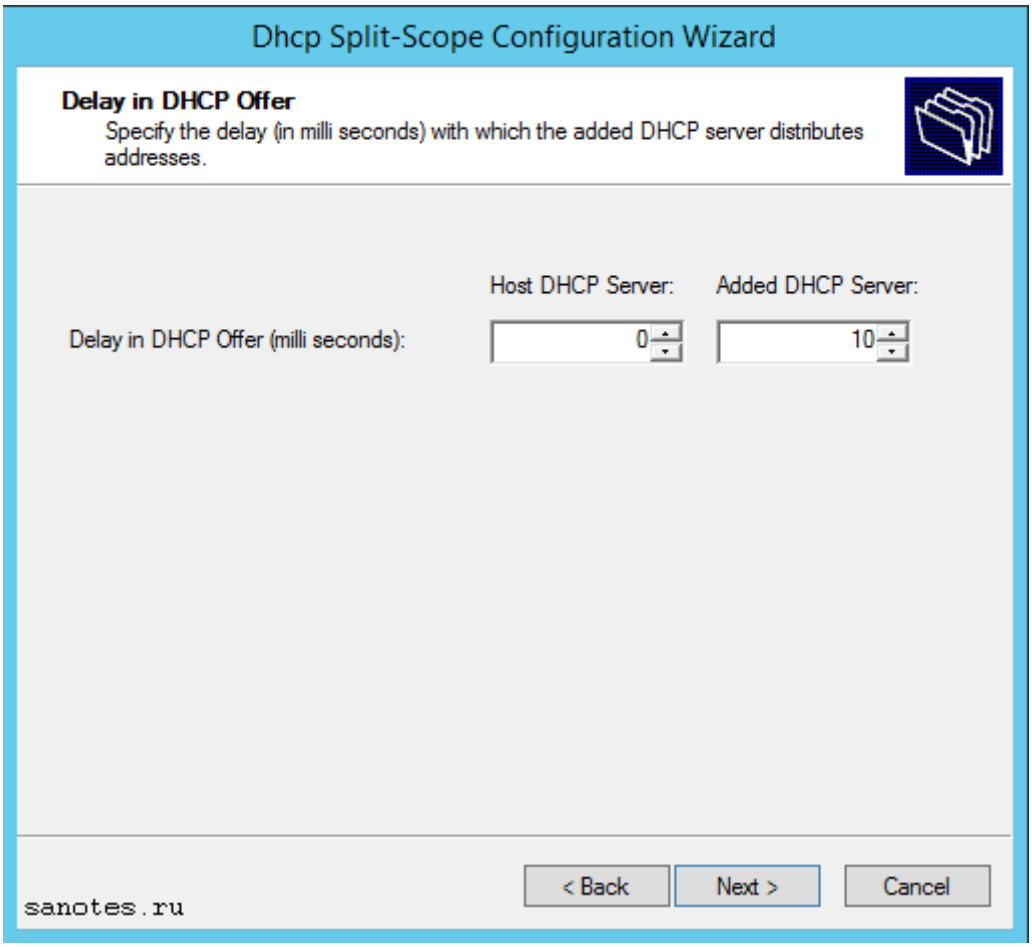



Затем двигая ползунок, отмечаем процентное соотношение распределения адресов в области. Жмем Далее.

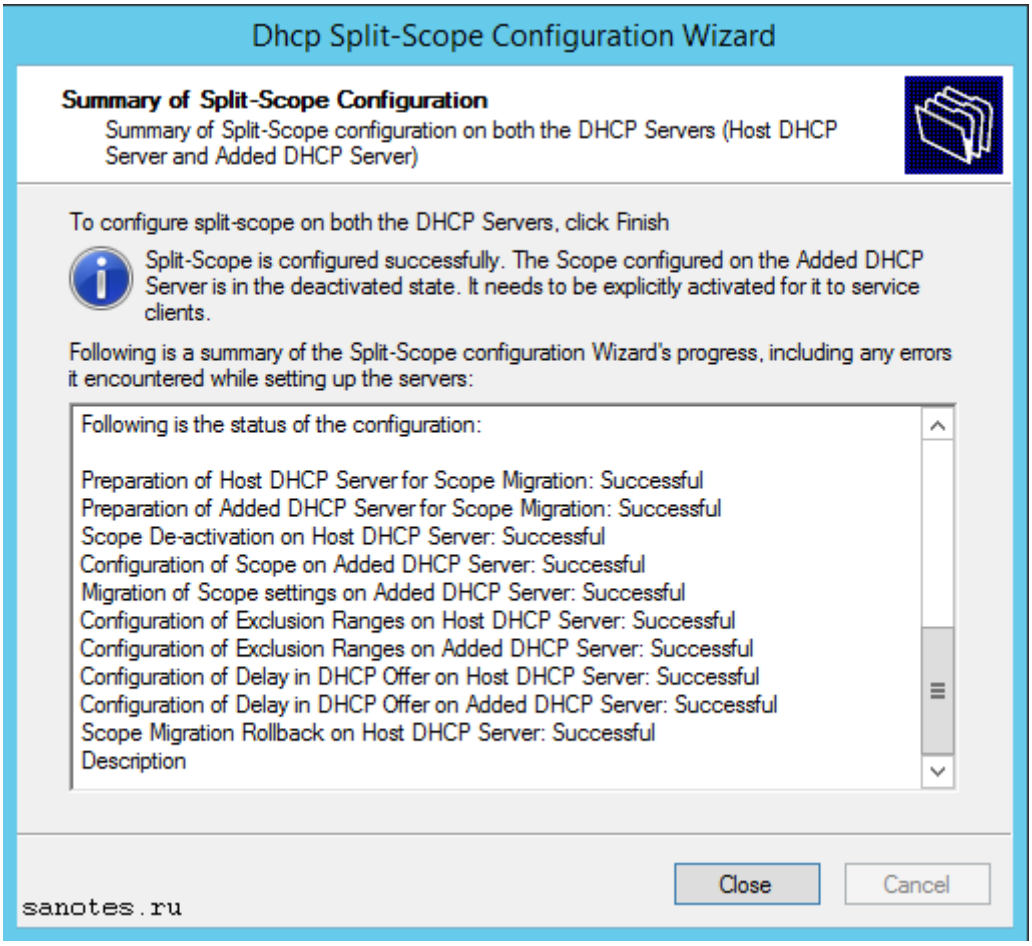



На следующем экране укажем задержку ответа серверов в мс. Укажем для второго сервера задержку в 10 мс, что позволит выдавать все адреса первым сервером, а второй только при

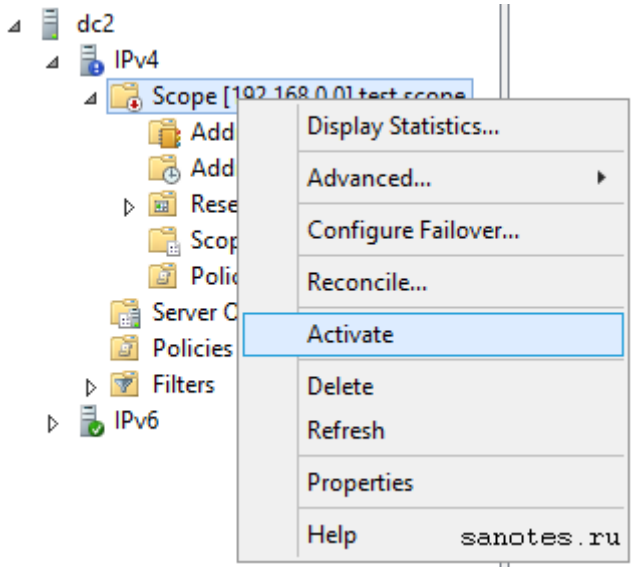
отказе первого или заполнении его пула адресов.




Жмем Next и наконец нажимаем Finish.



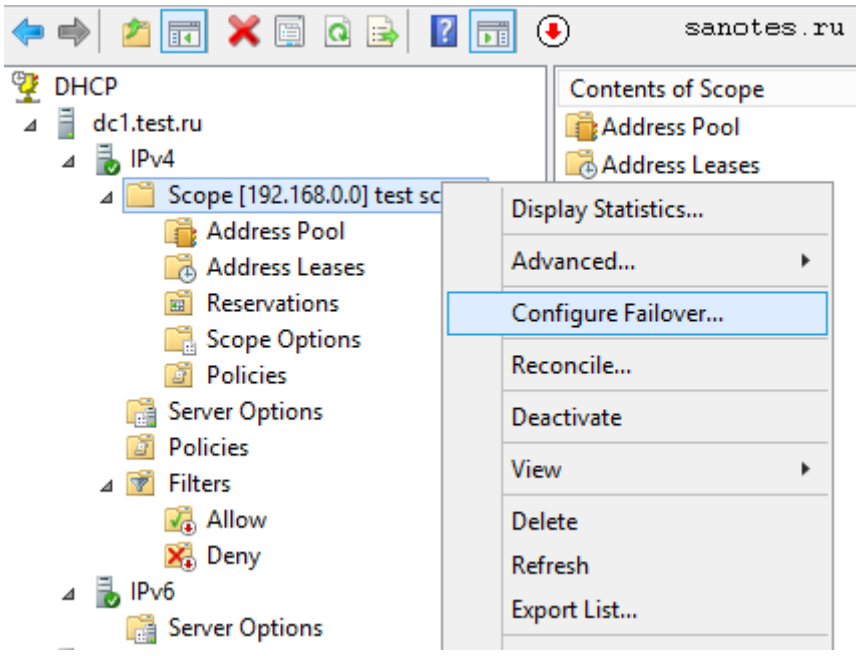
Затем нажимаем refresh на втором DHCP сервере, после чего увидим созданную область, где помимо основного диапазона с начальным и конечным адресом, будет диапазон адресов первого сервера исключенных для выдачи на втором сервере. Теперь, если видим что серверы обслуживают не пересекающиеся области, то можем активировать область на втором сервере.



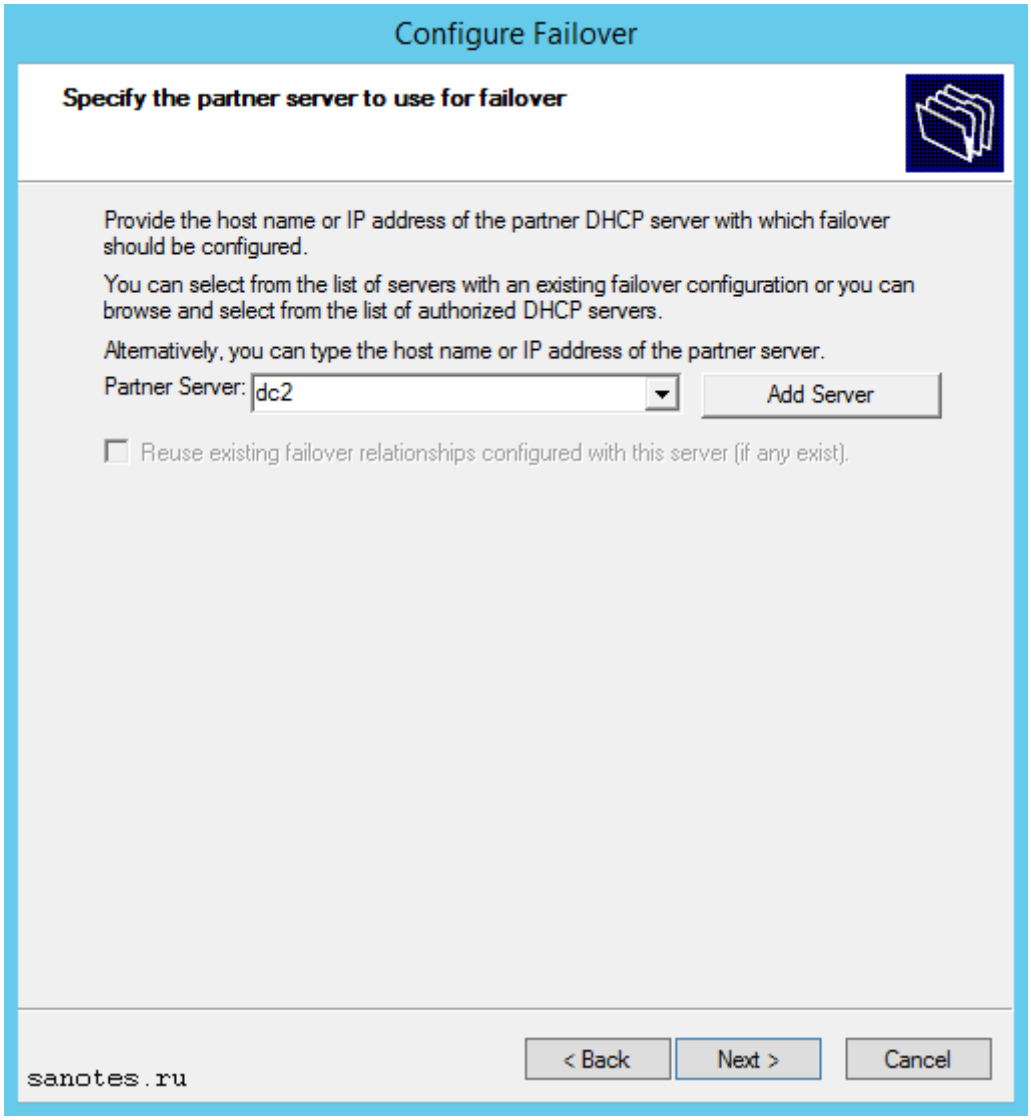

**2) DHCP с отработкой на отказ (DHCP Failover).** Новый механизм, появившийся в Windows Server 2012/R2. Второй DHCP сервер принимает нагрузку в случае отказа основного. Работает в двух режимах.

- **С балансировкой нагрузки (Load Balance Active-Active)**. При использовании этого режима два сервера одновременно предоставляют IP-адреса и сетевые параметры клиентам подсети. Запросы клиентов распределяются между двумя серверами согласно процентному соотношению заданному в Load Balance Percentage (по умолчанию 50 на 50).
- **Режим горячей замены (Hot Standby Active-Passive).** В этом режиме, один сервер (активный), отвечает за предоставление IP-адресов и параметров конфигурации всем клиентам в области или подсети, а дополнительный сервер (пассивный) принимает эту ответственность на себя в случае, если основной сервер становится недоступным. Сервер является основным или дополнительным в контексте подсети.

Для создания отношений отработки отказа между двумя DHCP-серверами, необходимо в оснастке DHCP щелкнуться правой кнопкой по имени области и выбрать Configure Failover.

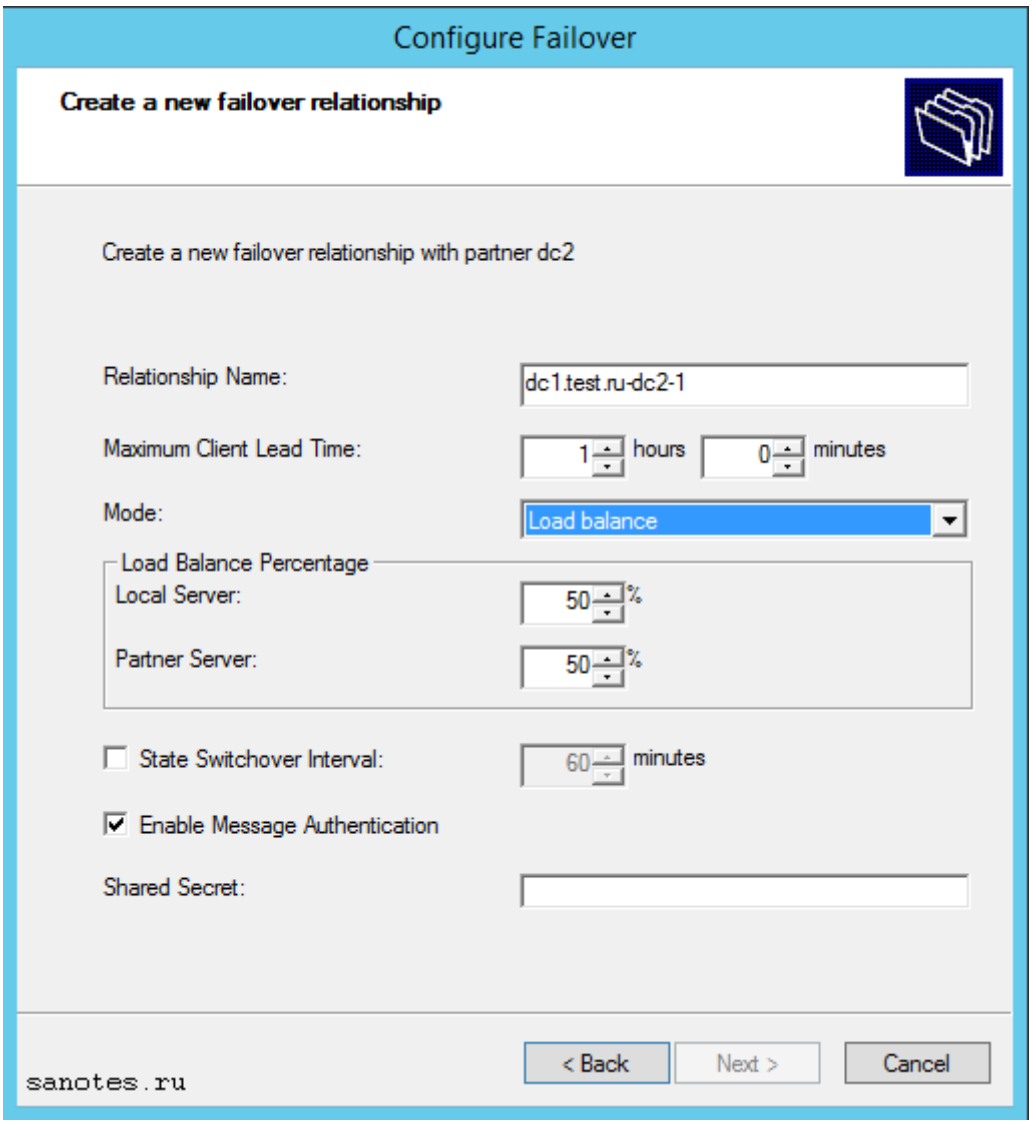



Затем нажимаем Next и следуем указаниям мастера. В поле Partner Server выберем второй сервер.




Галочка **Reuse existing failover relationships configured with this server (if any exist)** (Использовать существующие отношения отработки отказа с этим сервером (если доступно)) будет активна в том случае, если ранее мы уже создавали отношение отработки отказа, и мастер предложит воспользоваться существующей конфигурацией. Жмем Далее.

На следующем экране зададим параметры отношения отработки отказа:

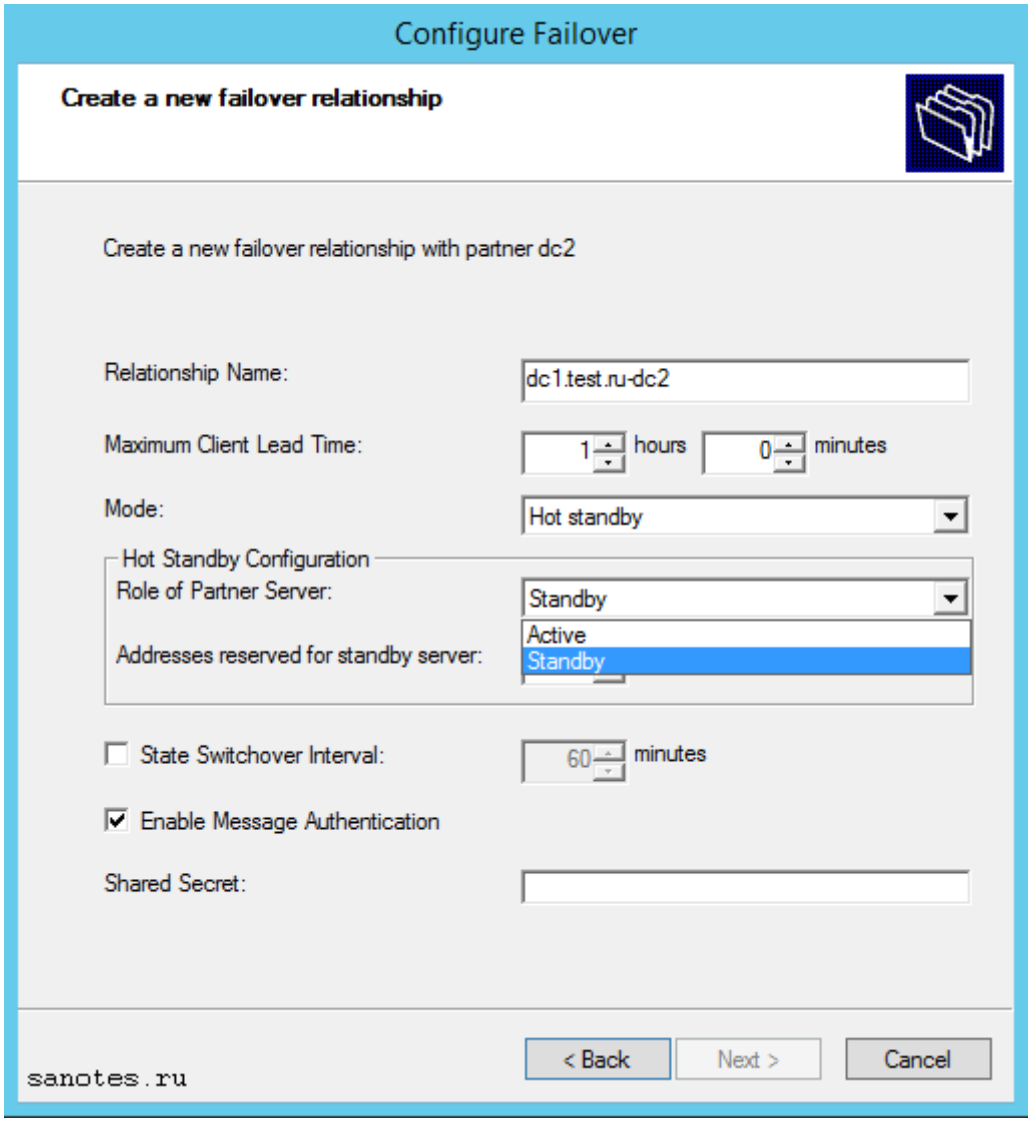



**Relationship Name** — уникальное имя конфигурации отношения отказа;

**Maximum Client Lead Time** — Максимальное время упреждения клиента (MCLT) — дополнительное время аренды IP-адреса выдаваемого доступным сервером для клиентов, которые должны быть обслужены тем сервером, который в данный момент недоступен;/p>

**Mode —** режим **Load Balance** (с балансировкой нагрузки) или **Hot Standby** (горячей замены).

В режиме **Hot Standby** (горячей замены) необходимо выбрать состояние работы сервера: Активный или Резервный и количество адресов в процентом отношении, которое резервируется для сервера горячей замены.

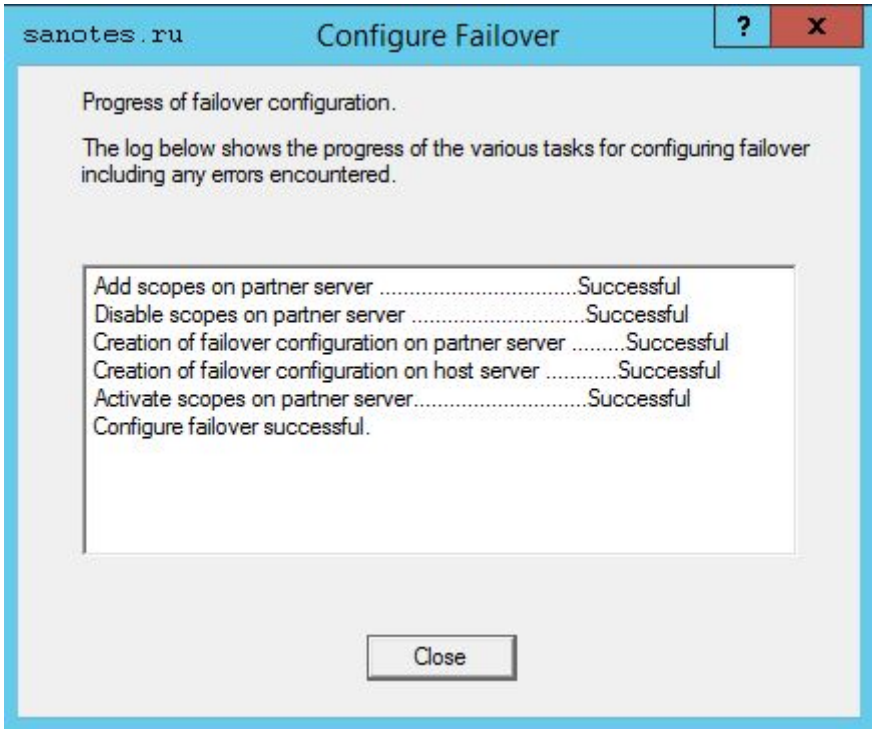



**Load Balance Percentage** — процентное отношение нагрузки между серверами участниками. По умолчанию 50 на 50.

**State Switchover Interval** — интервал времени, по истечении которого сервер DHCP автоматически переводит участника отработки отказа к партнеру после потери связи.

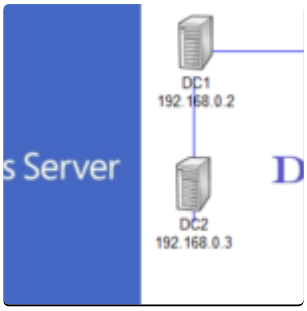
**Enable Message Authentication пароль Shared Secret,** используемый для взаимной, безопасной аутентификации серверов.

Выбираем режим по умолчанию **Load Balance**. Зададим пароль **Shared Secret**, остальные параметры оставим по умолчанию. Жмем Далее. Завершим настройку нажатием Finish и Close.

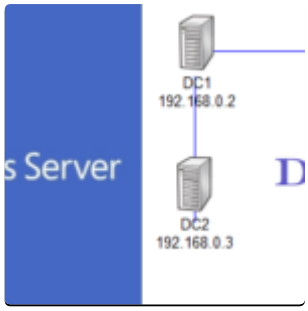



На этом установку второго контроллера домена (replica) и сопутствующих служб в существующем домене 'test.ru' можно считать завершенной. В следующей **заметке** будем поднимать филиальный домен только для чтения (RODC).

## Похожие статьи

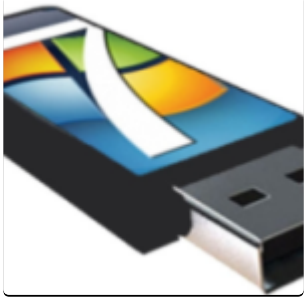



**Установка контроллера домена только для чтения (RODC) на базе Windows 2012 R2 (core)**

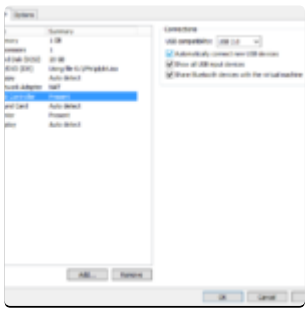



**Первый контроллер домена в лесу, на базе Windows 2012 R2. Настройка служб AD DS, DNS, DHCP**

**Dynamic registration or deletion of one or more DNS records associated with DNS domain 'domainname' failed.**



**Автоматическая установка настроенного образа Windows 7/2008R2 с usb-накопителя**



**Как загрузиться с usb-флешки на виртуальной машине**

30.03.15 | Просмотров: 10 661 | Метки: Active Directory, DHCP, DNS, domain controller, Windows | Категории: Windows