**Синхронизация времени в домене Windows Server 2008 R2**

На первом контроллере домена обязательно нужно настроить синхронизацию времени с внешним ntp-сервером.

В первую очередь надо открыть 123 udp порт для контроллера туда и обратно.  
  
1. Запускаем командную строку от имени администратора.  
2. Останавливаем службу W32Time:

net stop w32time

3. Задаем адреса источников времени:

w32tm /config /syncfromflags:manual /manualpeerlist:"0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org"

4. Теперь настроим контроллер на ответ клиентам на запросы о синхронизации времени:

w32tm /config /reliable:yes

5. Стартуем службу времени W32Time:

net start w32time

Проверка текущей конфигурации службы времени:

w32tm /query /configuration

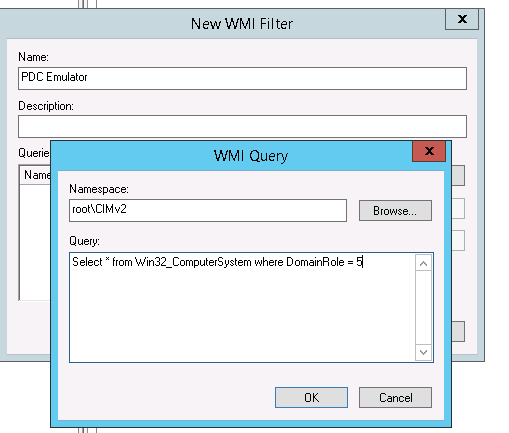
Можно ещё посмотреть журнал для проверки работоспособности.

Вручную запустите синхронизацию времени:  
w32tm /resync

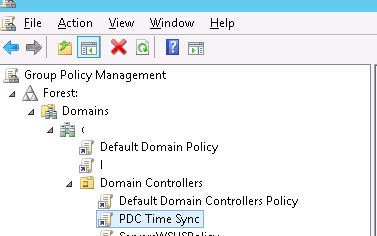
* Получение точного времени со всех серверов по протоколу Time (TCP порт 37)
* Получение точного времени со всех серверов по протоколу Daytime (TCP порт 13)

## **Настройка политики синхронизации NTP на контролере домена PDC**

Этот шаг предполагает настройку контроллера домена с ролью эмулятора PDC на синхронизацию времени с внешним NTP сервером. Т.к. теоретически роль эмулятора PDC может перемещаться между контроллерами домена, нам нужно сделать политику, которая применялась бы только к текущему владельцу роли PDC. Для этого в консоли управления **Group Policy Management Console** (GPMC.msc), создадим новый [WMI фильтр групповых политик](https://winitpro.ru/index.php/2012/01/13/filtraciya-gruppovyx-politik-s-pomoshhyu-wmi-filtrov/). Для этого в разделе **WMI Filters** создадим фильтр и именем **PDC Emulator** и WMI запросом: Select \* from Win32\_ComputerSystem where DomainRole = 5



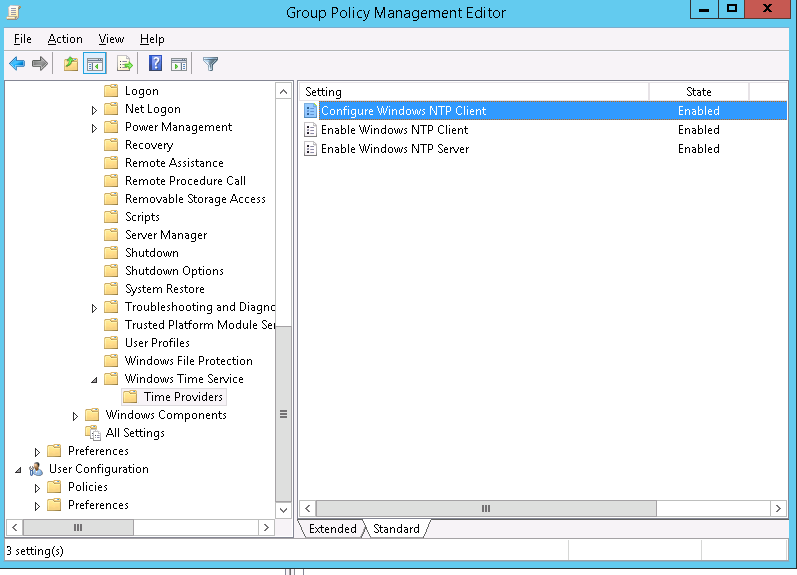
Затем создайте новую GPO и назначьте ее на контейнер Domain Controllers.



Перейдите в режим редактирования политики и разверните следующий раздел политик: **Computer Configuration->Administrative Templates->System->Windows Time Service->Time Providers**

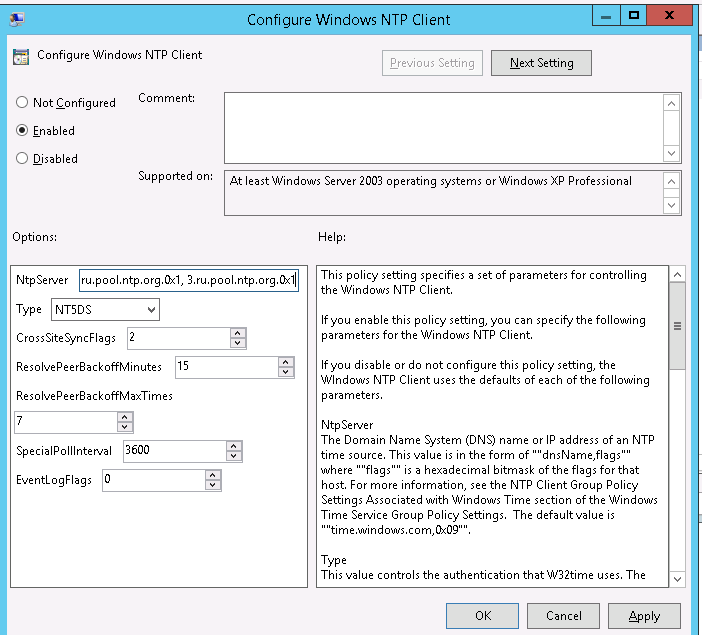
Нас интересуют три политики:

* **Configure Windows NTP Client**: Enabled (настройки политики описаны ниже)
* **Enable Windows NTP Client**: Enabled
* **Enable Windows NTP Server**: Enabled

  
В настройках политики Configure Windows NTP Client укажите следующие параметры:

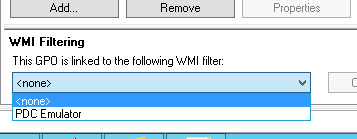
* **NtpServer**: 0.ru.pool.ntp.org,0x1 1.ru.pool.ntp.org,0x1 2.ru.pool.ntp.org,0x1 3.ru.pool.ntp.org,0x1
* **Type**: NTP
* **CrossSiteSyncFlags**: 2
* **ResolvePeerBackoffMinutes**: 15
* **Resolve Peer BAckoffMaxTimes**: 7
* **SpecilalPoolInterval**: 3600
* **EventLogFlags**: 0

**Совет**. Не забудьте настроить межсетевой экран таким образом, чтобы сервер PDC мог получить доступ к внешним NTP серверам по протоколу NTP (UDP порт 123).



**Примечание**. Обратите внимание на синтаксис в поле **NtpServer.**Формат указания нескольких NTP серверов такой:**ntsrv1.org,0x1 ntpsrv2.org,0x1**(разделитель пробел). На скриншоте указаны ошибочные данные!

Примените созданный ранее фильтр **PDC Emulator** к данной политике.



**Совет**. Найти имя сервера с ролью PDC можно с помощью команды: netdom query fsmo

Осталось обновить политики на контроллере PDC:  
gpupdate /force

Вручную запустите синхронизацию времени:  
w32tm /resync

Проверьте текущие настройки NTP:  
w32tm /query /status

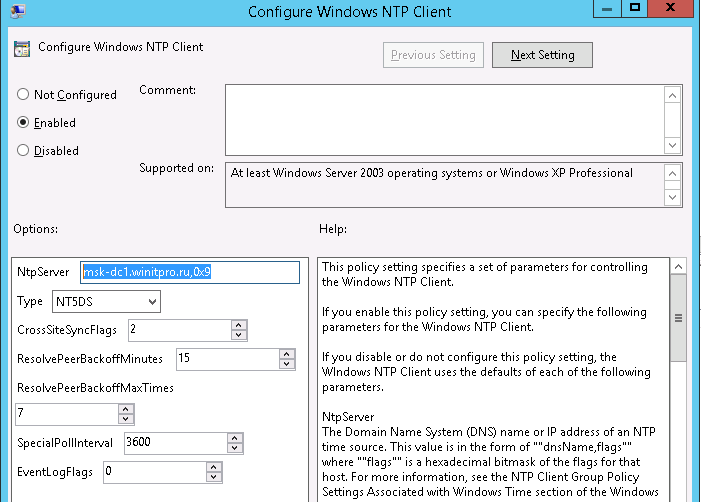
**Совет**. В том случае, если время не синхронизировалось, перезапустите службу времени Windows и сбросьте текущие настройки:  
net stop w32time  
w32tm.exe /unregister  
w32tm.exe /register  
net start w32time

## **Настройка синхронизации времени на клиентах домена**

В среде Active Directory по умолчанию клиенты домена синхронизируют свое время с контролерами домена (опция **Nt5DS** – синхронизировать время согласно иерархии домена). Как правило, эта схема работает и не требует перенастройки. Однако при наличии проблем с синхронизацией времени на клиентах домена, можно попробовать принудительно назначить сервер времени для клиентов с помощью GPO.

Для этого создайте новую GPO и назначьте ее на контейнеры (OU) с компьютерами. В редакторе GPO перейдите в раздел **Computer Configuration -> Administrative Templates -> System -> Windows Time Service -> Time Providers** и включите политику **Configure Windows NTP Client**.

В качестве сервера NTP укажите имя или ip адрес PDC, например msk-dc1.winitpro.ru,0x9, а в качестве типа синхронизации — NT5DS



[Обновите настройки групповых политик](https://winitpro.ru/index.php/2020/07/09/obnovlenie-gruppovyx-politik-windows/) на клиентах и проверьте, что клиенты успешно синхронизировали свое время с PDC.

**Совет**. Указанная схема применима только к небольшим доменам. Для больших распределенных доменов с большим количеством DC и сайтов придется создать отдельную политику для каждого сайта, чтобы клиенты синхронизировали свое время с DC в сайте.