Службы синхронизации времени в ОС Astra Linux

Инструкция по быстрой настройке клиента синхронизации времени на клиентском компьютере:

```
sudo apt remove ntp
sudo timedatectl set-ntp true
sudo systemctl start systemd-timesyncd
```

Проверка результата:

```
sudo systemctl status systemd-timesyncd
```

Подробности ниже в статье: Служба TIMESYNCD

Данная статья применима к:

- ОС ОН Орёл 2.12;
- ОС СН Смоленск 1.6;
- ОС СН Ленинград 8.1.

Системы электронной цифровой подписи (ЭЦП) для поставления отметок времни на подписываемых документах используют свои собственные доверенные серверы времени. Настройка этих серверов должна осуществляться в соответствии с инструкциями поставщиков таких систем.

В стандартные дистрибутивы ОС ОН Орёл 2.12 и ОС СН Смоленск 1.6 и Ленинград 8.1 включены три службы точного времени:

- **Серверная служба NTP** (представлена пакетами ntp и ntpdate). Может обеспечивать работу ОС в режиме как сервера точного, так и клиента.

  Для синхронизации времени с внешними серверами служба **ntp** требует полного двустороннего доступа к сетевому порту 123 и не умеет работать с другими портами. Если по каким-то причинам порт 123 в вашей сети закрыт и не может быть открыт, то возможно применение одного из следующих решений:
  - Использовать локальные аппаратные источники точного времени;
  - Выносить службу ntp на сервер межсетевого экрана, чтобы она имела открытый порт 123 с выходом в Интернет;
  - Использовать ручную или автоматическую принудительную коррекцию времени с помощью команды ntpdate (см. ниже);
  - Использовать службу **systemd-timesyncd** (см. ниже);

- **Клиентская служба timedatectl / systemd-timesyncd.service**. Не представлена отдельными пакетами, встроена непосредственно в ОС.
  Предназначена для использования только на клиентских ОС, и не может работать сервером точного времени.
  Поддерживает только упрощенный протокол передачи времени, однако считается более современным вариантом для типичных клиентских применений.

  Служба **systemd-timesyncd.service** не будет работать, если:
  - Обнаружит на компьютере установленную службу NTP (даже незапущенную);
  - Обнаружит на компьютере установленные гостевые дополнения Oracle Virtual Box (предполагается, что на виртуальных машинах синхронизацию времени выполняет менеджер виртуальных машин).

- **Служба времени высокой точности PTP (Precision Time Protocol)** - описание представлено в отдельной статье.

Службы ntp и timesyncd несовместимы между собой и их одновременная работа невозможна.

Служба timesyncd отказывается работать на виртуальный машинах. Современные системы виртуализации сами обеспечивают синхронизацию часов виртуальной машины с часами физической машины.

Основные понятия

При работе с часами используются следующие понятия, связанными друг с другом через параметры временной зоны и настроек аппаратных часов:

Тип	Пояснение	Пример
Universal time, UTC	**UTC** — это всемирное координированное время, стандарт времени, принятый на Земле. От **UTC** отсчитываются часовые пояса. **UTC** заменил устаревшее время по Гринвичу (GMT). **UTC** расшифровывается как Coordinated Universal Time (по-английски) или Temps universel coordonné (по-французски). Так как не зависит от местоположения компьютера, используется в качестве системного времени: времени в ядре ОС, для отметок времени для записи журналов, и для синхронизации времени службами времени.	Universal time: Ср 2019-02-20 07:51:49 UTC
Time Zone	Временная зона. Определяет временное смещение и параметры сезонного (зимнего/летнего) времени.	Time zone: Europe/Moscow (MSK, +0300)
Local time	Локальное время, местное время. Получается из всемирного координированного времени добавлением временного смещения, определённого во временной зоне. Для Москвы смещение составляет +3 часа (Time zone: Europe/Moscow (MSK, +0300)). Используется в основном для взаимодействия с пользователями системы.	Local time: Ср 2019-02-20 10:51:49 MSK
RTC time	Аппаратное время. Время, установленное в аппаратных часах компьютера (Real Time Clock, RTC, также CMOS или BIOS time). Используется для первоначальной установки времени при загрузке ОС. Аппаратные часы могут быть настроены как на всемирное координированное, так и на местное время. При установке системного времени (UTC) на основании показаний аппаратных часов (UTC или местное) операционная система принимает решение о том, какое именно время (UTC или местное) показывают аппаратные часы, на основании собственных внутренних настроек (см. man timedatectl). ⚠ Аппаратные часы рекомендуется всегда использовать в режиме UTC. Если на компьютере установлены несколько операционных систем, то во всех этих операционных системах должны быть выставлены одинаковые параметры интерпретации показаний системного времени. Современные установщики Linux-систем при установке ОС считают, что аппаратные часы работают в режиме UTC. Все установщики Windows считают, что аппаратные часы работают в режиме **локального времени**. Если на компьютере одновременно установлены несколько операционных систем, то во всех этих операционных системах должны быть выставлены одинаковые параметры интерпретации показаний системного времени. В версии Astra Linux ОС СН Смоленск 1.5 установщики для совместимости в Windows был настроен трактовать показания времени RTC как показания локального времени. Так как использование RTC в режиме локального времени неудобно при работе географически распределённых доменных систем, установщики Astra Linux начиная с версий ОС ОН Орёл 2.12 и ОС СН Смоленск 1.6 считают, что аппаратные часы работают в режиме UTC.	RTC time: Ср 2019-02-20 07:51:49 ⊘ Следует помнить, что некоторые аппаратные платформы (например, Raspberry Pi) не оборудованы энергонезависимыми аппаратными часами, и в них показания аппаратного времени должны быть выставлены после включения программно операционной системой.

Служба времени NTP

Эта служба устанавливается при установке ОС Astra Linux, однако, в зависимости от используемой версии ОС может автоматически не запускаться.

Проверить статус службы можно командой:

```
sudo systemctl status ntp
```

Если служба не запущена, всключить её автоматический запуск при старте компьютера и запустить её можно командами:

```
sudo systemctl enable ntp
sudo systemctl start ntp
```

После запуска, в общем случае, для использования в качестве клиентской службы, дополнительных настроек не требует.

Настроенная на автоматический запуск при перезагрузке компьютера служба ntp будет запускаться автоматически, но, если она не сможет найти ни одного сервера времени из перечисленных в её конфигурации, то будет так же автоматически прекращать свою работу.

Для управления службой в состав дистрибутивов включен графический инструмент fly-admin-ntp, который можно установить из графического менеджера пакетов, или из командной строки:

```
sudo apt install fly-admin-ntp
```

После установки графического инструмента он будет доступен в меню:

Пуск -> Панель управления -> Сеть -> Синхронизация времени (NTP).

Описанные далее действия по настройке можно выполнять с помощью графического инструмента,
или непосредственно редактировать файл настроек `/etc/ntp.conf`.

Свой сервер времени

При настройках "по умолчанию" служба ntpd выдает отметки времени всем, кто их запросит, но никому не разрешает управлять собой удалённо.

Пример файла конфигурации службы NTP (/etc/ntp.conf):

```
# /etc/ntp.conf, configuration for ntpd; see ntp.conf(5) for help

driftfile /var/lib/ntp/ntp.drift

# Enable this if you want statistics to be logged.
#statsdir /var/log/ntpstats/

statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable


# You do need to talk to an NTP server or two (or three).
#server ntp.your-provider.example

# pool.ntp.org maps to about 1000 low-stratum NTP servers. Your server will
# pick a different set every time it starts up. Please consider joining the
# pool: <http://www.pool.ntp.org/join.html>
pool 0.debian.pool.ntp.org iburst
pool 1.debian.pool.ntp.org iburst
pool 2.debian.pool.ntp.org iburst
pool 3.debian.pool.ntp.org iburst


# Access control configuration; see /usr/share/doc/ntp-doc/html/accopt.html for
# details. The web page <http://support.ntp.org/bin/view/Support/AccessRestrictions>
# might also be helpful.
#
# Note that "restrict" applies to both servers and clients, so a configuration
# that might be intended to block requests from certain clients could also end
# up blocking replies from your own upstream servers.
```

```
# By default, exchange time with everybody, but don't allow configuration.
restrict -4 default kod notrap nomodify nopeer noquery limited
restrict -6 default kod notrap nomodify nopeer noquery limited

# Local users may interrogate the ntp server more closely.
restrict 127.0.0.1
restrict ::1

# Needed for adding pool entries
restrict source notrap nomodify noquery

# Clients from this (example!) subnet have unlimited access, but only if
# cryptographically authenticated.
#restrict 192.168.123.0 mask 255.255.255.0 notrust


# If you want to provide time to your local subnet, change the next line.
# (Again, the address is an example only.)
#broadcast 192.168.123.255

# If you want to listen to time broadcasts on your local subnet, de-comment the
# next lines.  Please do this only if you trust everybody on the network!
#disable auth
#broadcastclient
```

Все подключения к службе ограничены, а управляющие подключения запрещены:

```
# ограничения для IPv4
restrict -4 default kod notrap nomodify nopeer noquery limited

# ограничения для IPv6
restrict -6 default kod notrap nomodify nopeer noquery limited
```

По умолчанию заданы следующие параметры ограничений:

- kod — узлам, которые слишком часто отправляют запросы сначала отправить предупреждение (поцелуй смерти, kiss of death), затем отключить от сервера
- notrap — не принимать управляющие команды
- nomodify — не принимать команды, которые могут вносить изменения состояния
- nopeer — не синхронизироваться с хостом
- noquery — не принимать запросы
- limited — ограничение одновременного приема запросов

При этом управление с локального компьютера разрешено, и по необходимости можно добавить более слабые ограничения. Например, для сети 192.168.0.0

```
# не запрещаем принимать запросы от сети 192.168.0.0, но не разрешаем управление из этой сети
restrict 192.168.0.0 mask 255.255.255.0 nomodify notrap

# разрешаем управление с локального компьютера
restrict 127.0.0.1
restrict ::1
```

Так как сервер времени сам выступает клиентом для получения своего точного времени, настройка источников синхронизации для сервера делается так же, как и для клиента.

После внесения изменений в конфигурацию следует перезапустить сервис:

```
sudo service ntp restart
```

Контроль состояния сервиса NTP

Для контроля состояния сервиса NTP предусмотрена команда ntpq, входящая в пакет сервера.
Эта команда получает состояние сервиса с помощью стандартных запросов и выводит сводку на печать.
Типичный вызов команды:

```
ntpq -duv
```

При этом опция -d запрещает корректировать время, опция -u позволяет отправить запрос через непривилегированный IP-порт, а не через порт 123, чтобы избежать конкуренции со службой ntpd, -v - подробный отладочный вывод.

Типичный вывод команды при нормально работающем сервисе:

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 0.ru.pool.ntp.o .POOL.          16 p    -   64    0    0.000    0.000   0.000
 1.ru.pool.ntp.o .POOL.          16 p    -   64    0    0.000    0.000   0.000
 2.ru.pool.ntp.o .POOL.          16 p    -   64    0    0.000    0.000   0.000
 3.ru.pool.ntp.o .POOL.          16 p    -   64    0    0.000    0.000   0.000
 127.127.1.0     .LOCL.          10 l 1101   64    0    0.000    0.000   0.000
+185.209.85.222  195.91.239.8     2 u   20   64  377   10.631    0.690   0.355
*195.91.239.8    .PPS.            1 u   19   64  377    1.256    0.081   0.065
+192.36.143.130  .PPS.            1 u   18   64  377   19.755    0.129   0.330
-37.193.156.169  80.242.83.227    2 u   12   64  377   44.877   -0.832   2.427
-95.165.138.248  89.109.251.24    2 u    7   64  377    3.118    0.241   0.140
```

Где:

- первый символ в строке - статус выбора:
  - ***** — выбранный север времени;
  - **+** — новый сервер;
  - **o** — PPS-источник (источник секундных импульсов);
  - пробел — не работающий источник;
  - **— x** и др. — «забракованные» (ненадежные) источники.
- remote - адрес опрошенного сервера времени;
- refid - источник сигналов времени, с которым синхронизируется опрошенный сервер.
  Это может быть другой сервер, а могут быть аппаратные часы.
  В приведённом примере видно, что серверы первого стратума синхронизируются по аппаратным часам;
- st - уровень (стратум) сервера. Может принимать значения от 0 до 16. Чем ниже уровень - тем точнее сервер.
  Значение стратума 16 скорее всего говорит о том, что сервер признан негодным источником;
- t - тип сервера (u - unucast, m - multicast, l - local, p - pool и т.д.);
- when - время, прошедшее с последней синхронизации (последнего ответа сервера), в секундах, если не указано иное;
- poll - интервал опроса (двоичный логарифм периода опроса в секундах);
- reach - восьмеричное значение сдвигового регистр доступности.
  Отражает доступность сервера при последних восьми опросах, при 100% доступности проходит значения 0, 1, 3, 7, 17, 37, 77, 177, 377 и далее остаётся равным 377;
- delay - задержка ответа (время между отправкой запроса и получением ответа);
- offset - смещение времени относительно локального сервера;
- jitter- дисперсия (разброс) времени прохождения пакетов при обмене с сервером

Типичные ошибки, которые можно обнаружить с помощью этой команды:

- no server suitable for synchronization found - говорит сама за себя, типично для службы ntpd, которая, не обнаружив возможности синхронизироваться, просто перестайт
- leap not in sync - сервер находится в состоянии незавершенной коррекции времени, его показания пока недостоверны. Обычно исчезает через некорое время, после завершения синхронизации.

Принудительная коррекция времени с помощью команды ntpdate

Для коррекции показаний времени в составе дистрибутивов предусмотрен инструмент командной строки ntpdate.
Этот же инструмент может испоьзоваться для периодической коррекции времени (например, с помощью службы cron).

Он не устанавливается по умолчанию, и может быть установлен с помощью графического менеджера пакетов или из командной строки командой

```
sudo apt install ntpdate
```

Типичные применения:

- проверка доступности сервера времени запросом времени без коррекции показаний времени (опция -q):

```
sudo ntpdate -q 0.ru.pool.ntp.org

#

sudo ntpdate -qu 0.ru.pool.ntp.org
```

По умолчанию ntpdate использует тот же IP-порт (123) что и ntpd, и, если сервис ntpd запущен, то ntpdate при запуске сообщает, что порт занят:

```
sudo ntpdate -q 0.ru.pool.ntp.org
```

```
ntpdate[1421]: the NTP socket is in use, exiting
```

Так как IP-порт 123 часто закрыт по соображениям безопасности, команду ntpdate БЕЗ опции -u можно использовать для проверки доступности внешних серверов времени для службы ntpd (запросы в этом случае следует отправлять на серверы времени, указанные в конфигурационном файле службы ntpd):

```
sudo service ntp stop
sudo ntpdate -q 0.ru.pool.ntp.org
sudo service ntp start
```

- Команда ntpdate может применяться для периодической коррекции времени:

```
sudo ntpdate -ubv 0.ru.pool.ntp.org
```

См. тж. про применение ntpdate в статье про виртуализацию

Передача параметров NTP через DNS

Параметры для доступа к NTP могут автоматически передаваться клиентам через DNS-сервер.
Подробности см. в DNS-сервер BIND9

Изменение настроек клиентов

Изменение настроек может понадобиться в следующих ситуациях:

- оптимизация и локализация сетевого трафика
- работа в изолированной сети
- работа со специальными серверами времени

По умолчанию, служба настроена на работу с открытым пулом специальных серверов времени,
выбирая при запуске каждый раз новый оптимальный набор серверов со всего мира:

```
pool 0.debian.pool.ntp.org iburst
pool 1.debian.pool.ntp.org iburst
pool 2.debian.pool.ntp.org iburst
pool 3.debian.pool.ntp.org iburst
```

Для того, чтобы служба NTP могла обращаться к серверам, имена которых заданы в текстовом виде (как в примере выше), необходимо, чтобы был настроен и работал сервис разрешения имён DNS.
Если служба DNS отсутствует, серверы времени должны быть заданы в виде IP-адресов.
Независимо от способа указания серверов времени, если служба DNS в очередном цикле опроса не сможет обратиться ни к одному из указанных в конфигурационном файле серверов, она просто аварийно завершит свою работу.

При желании ограничить набор серверов российскими серверами можно использовать следующие настройки:

```
pool 0.ru.pool.ntp.org iburst
pool 1.ru.pool.ntp.org iburst
pool 2.ru.pool.ntp.org iburst
pool 3.ru.pool.ntp.org iburst
```

Кроме того, можно использовать серверы ВНИИФТРИ, актуальный список которых доступен по ссылке: http://vniiftri.ru/ru/uslugi-serverov

При необходимости работать в изолированной сети, или при желании ограничить свой внешний трафик, можно использовать свои локальные серверы времени:

server <IP_адрес_сервера_1>
server <IP_адрес_сервера_2>

Особенности работы в виртуальных машинах

Некоторые особенности синхронизации времени описаны в статье про виртуализацию

Служба TIMESYNCD

Служба timesyncd предлагается в качестве современной "легковесной" замены ntp.
Она более проста, интегрирована в ОС, но несколько ограничена в возможностях.

Служба TIMESINCD не может выполнять функции сервера, это исключительно клиентская служба.

Служба timesyncd устанавливается автоматически при установке ОС , автоматически запускается при каждой перезагрузке ОС, однако немедленно завершает свою работу с сообщением об ошибке, обнаружив, что на компьютере присутствует служба ntp.

Отключить невостребованный автоматический запуск службы можно командой:

```
sudo timedatectl set-ntp false
```

Включить, соответственно, командой (однако, пока присутствует служба NTP, служба TIMESYNCD всё равно работать не будет):

```
sudo timedatectl set-ntp true
```

Для использования timesyncd в первую очередь необходимо полностью удалить службу ntp:

```
sudo apt remove ntp
```

После чего запустить службу timesyncd:

```
sudo systemctl start systemd-timesyncd
```

Состояние службы можно проверить командой:

```
sudo systemctl status systemd-timesyncd
```

Или командой:

```
sudo timedatectl status
```

Примерный вывод команды:

```
      Local time: Ср 2018-12-26 11:08:12 MSK
  Universal time: Ср 2018-12-26 08:08:12 UTC
        RTC time: Ср 2018-12-26 08:08:12
       Time zone: Europe/Moscow (MSK, +0300)
 Network time on: yes
NTP synchronized: yes
 RTC in local TZ: no
```

Выбор серверов времени

Служба TIMESYNCD по умолчанию скомпилирована для работы с набором серверов времени из пула Debian.

Дополнительно служба TIMESYNCD получает имена серверов времени от службы systemd-networkd, если служба systemd-networkd предоставляет такую информацию, т.е. в конфигурационных файлах этой службы (каталоги /lib/systemd/network/, /run/systemd/network/, /etc/systemd/network/ или файл /lib/) указаны серверы NTP, привязанные к сетевым интерфейсам (подробнее см. man systemd.network).

Дополнительные и резервные серверы могут быть указаны в собственных конфигурационных файлах службы TIMESYNCD

/etc/systemd/timesyncd.conf
/etc/systemd/timesyncd.conf.d/*.conf
/run/systemd/timesyncd.conf.d/*.conf
/usr/lib/systemd/timesyncd.conf.d/*.conf

Опции в конфигурационном файле:

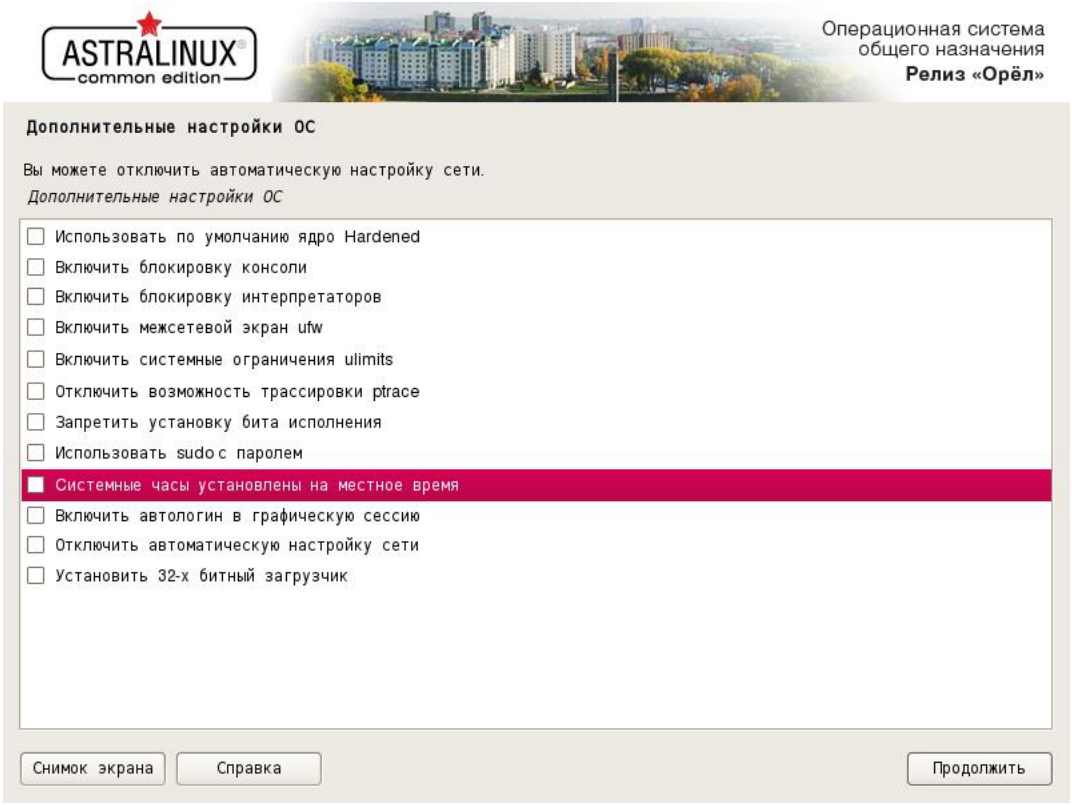
- NTP= - разделённый пробелами основной список имён NTP-серверов. Объединяется со списком полученных от службы systemd-networkd. По умолчанию список пустой.
- FallbackNTP= разделённый пробелами список имён резервных NTP-серверов.

TIMESYNCD перебирает по очереди все серверы из основного списка, и, если не удалось связаться ни с одним из серверов, обращается к серверам из резервного списка.

Настройка режима интерпретации показаний аппаратных (RTC) часов

При установке ОС

При установке ОС ОН Орёл 2.12 режим интерпретации показаний аппаратных часов можно выбрать в окне "Дополнительные настройки ОС", пункт "Системные часы установлены на местное время":



На установленной ОС

При использовании любой службы времени рекомендуется настраивать аппаратные часы компьютера так, чтобы они показывали не локальное, а всемирное координированное время (UTC).
Если этого не сделать, возможны проблемы с коррекцией времени и сменой сезонного локального времени.
Если RTC настроены на локальное время, команда timedatectl status будет выдавать соответствующее предупреждение.

Переключение аппаратных часов на время UTC с одновременной их синхронизацией с системным временем выполняется командой:

```
sudo timedatectl  set-local-rtc 0
```

Для переключения с одновременной синхронизацией системного времени по показаниям часов RTC можно использовать опцию --adjust-system-clock.

Переключение аппаратных часов на локальное время можно выполнить командой:

```
sudo timedatectl  set-local-rtc 1
```

Настройка режима интерпретации RTC в Windows

Если на компьютере установлены несколько операционных систем, то во всех этих операционных системах должны быть выставлены одинаковые параметры интерпретации показаний системного времени.

Чтобы ОС семейства Windows трактовали показания аппаратных часов как время UTC, использовать параметр реестра [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation] "RealTimeIsUniversal", установив его в единицу:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation] "RealTimeIsUniversal"=dword:00000001

или

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation] "RealTimeIsUniversal"=qword:00000001