

Ускорение авторизации доменных пользователей.

- [Вариант 1. Установка обновления безопасности.](#)
- [Вариант 2. Ручное исправление параметров кэша.](#)

При длительной работе некоторых приложений на серверах ОС CH Смоленск 1.5, находящихся в составе домена ALD, может наблюдаться замедление авторизации доменных пользователей, при этом мониторинг системы показывает, что доменная служба slapd (ldap-сервер) создаёт очень высокую загрузку процессора.

Данная ситуация может возникать при работе в доменной структуре приложений, использующих связку Apache2 — PostgreSQL в условиях мандатного контроля доступа.

Система мандатного контроля доступа обеспечивает выполнение особых требований к защите кешируемых данных с мандатными атрибутами безопасности пользователей.

По умолчанию, доступ к этим данным имеют только администратор (суперпользователь), и конкретный пользователь - владелец кэша.

Доступ сервисам, работающим от имени других системных учетных записей (например, учетные записи www-data или postgres) по умолчанию запрещен, что вызывает рассогласование обмена кешированными данными.

В результате, PostgreSQL перестает использовать кешированные данные пользователей, и запрашивает информацию непосредственно у ldap-сервера, создавая этим значительный сетевой трафик и повышенную нагрузку на сервер.

Для предотвращения вышеописанной проблемы нужно выполнить следующие действия:

Вариант 1. Установка обновления безопасности.

1. Установить на контроллер домена последнее обновление безопасности для используемой ОС, доступное на <http://astralinux.ru/update> ;
2. В конфигурационный файл /etc/ald/ald.conf добавить параметр CACHE_ACCESS_USERS с перечислением через запятую без пробелов имен пользователей, которые должны работать с файлами кэша, например:

```
CACHE_ACCESS_USERS=www-data,postgres
```

Для обеспечения нормальной работы службы PostgreSQL достаточно добавить только одного пользователя postgres:

```
CACHE_ACCESS_USERS=postgres
```

3. После внесения изменений в файл конфигурации перезапустить службу:

```
sudo service aldd restart
```

Вариант 2. Ручное исправление параметров кэша.

В случаях, когда установка обновлений безопасности по каким-то причинам невозможна, параметры кэша можно исправить, выполнив из командной строки следующую последовательность команд:

```
setfacl -d -m u:postgres:r /var/lib/ald/cache/parsec
setfacl -R -m u:postgres:r /var/lib/ald/cache/parsec
setfacl -m u:postgres:rx /var/lib/ald/cache/parsec
```