TERMIDESK

РУКОВОДСТВО АДМИНИСТРАТОРА

СЛЕТ.10001-01 90 07

Версия 5.1. Выпуск от ноября 2024

Настройка компонента «Сервер терминалов»

ОГЛАВЛЕНИЕ

1 . ОБЩИЕ СВЕДЕНИЯ

1.1 . О документе

Настоящий документ является седьмой частью руководства администратора на программный комплекс «Диспетчер подключений виртуальных рабочих мест Termidesk» (далее - Termidesk). Документ предназначен для администраторов системы и сети.

В этом руководстве приведено назначение, установка и настройка компонента «Сервер терминалов Astra Linux». Для того, чтобы получить информацию о месте компонента в программном комплексе, необходимо обратиться ко второй части руководства администратора - СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

1.2 . Назначение компонента «Сервер терминалов Astra Linux»

Компонент «Сервер терминалов Astra Linux» (англ. «Terminal Server Astra Linux», далее - STAL, сервер терминалов Astra Linux) входит в состав Termidesk.

STAL обеспечивает подключение пользовательских рабочих станций к рабочим местам (РМ) с операционной системой (ОС) Astra Linux Special Edition через сеанс удаленного терминала.

STAL позволяет выполнять доставку как рабочего стола РМ с ОС Astra Linux Special Edition, так и опубликованных приложений.

STAL устанавливается на узел, выбранный в качестве терминального сервера, совместно с компонентом «Сессионный агент» из состава Termidesk.

> ⚠ Для работы со STAL в политиках фонда РМ параметру «Механизм обеспечения безопасности на уровне сети (RDP)» должно быть задано значение «TLS» или «RDP» (см. подраздел **Политики фонда рабочих мест** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»).

1.3 . Требования к программному и аппаратному обеспечению

Для установки STAL минимальные аппаратные требования узла должны соответствовать следующим:

- процессор архитектуры Intel x86 разрядности 64 бит;
- оперативная память, не менее 2 ГБ;
- свободное дисковое пространство, не менее 200 МБ;
- сетевое соединение, не менее 100 Мбит/с.

STAL устанавливается на ОС:

- Astra Linux Special Edition (Server) 1.7 (версии 1.7.5.9, 1.7.6.14);

- Astra Linux Special Edition (Server) 1.8 (версия 1.8.1).

ОС должна быть установлена с графическим интерфейсом.

1.4 . Типографские соглашения

В настоящем документе приняты следующие типографские соглашения:

- моноширинный шрифт – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

2 . УСТАНОВКА И УДАЛЕНИЕ КОМПОНЕНТА

2.1 . Получение пакетов установки в ОС Astra Linux Special Edition

Дистрибутив представлен бинарным файлом пакета ПО в `deb`-формате. Установка в ОС Astra Linux Special Edition производится из локального репозитория, распространяемого в формате `iso`-образа.

Получить `iso`-образ можно двумя способами:

- заполнив запрос через сайт Termidesk: https://termidesk.ru/support/#request-support;
- через личный кабинет: https://lk-new.astralinux.ru/.

Для подключения локального репозитория Termidesk на узле, где предполагается установка, нужно:

- скопировать в домашний каталог пользователя образ диска `termidesk-<версия>.iso`;
- подключить образ диска к файловой системе в каталог `/mnt`:

```
sudo mount -o loop termidesk-<версия>.iso /mnt
```

где:

`-o loop` - параметры для привязки петлевого устройства (`/dev/loop`) к файлу `termidesk-<версия>.iso`, устройство затем монтируется в указанный каталог `/mnt`;

- скопировать содержимое каталога `repos` подключенного образа диска в каталог `/var` локальной файловой системы:

```
sudo cp -Rp /mnt/repos /var
```

где:

`-Rp` - ключ для рекурсивного копирования подкаталогов и файлов с сохранением исходных свойств;

- отключить подключенный ранее образ диска от узла:

```
sudo umount /mnt
```

- установить пакет `lsb-release`:

```
sudo apt install -y lsb-release
```

где:

`-y` - ключ для пропуска подтверждения установки;

- добавить локальный репозиторий Termidesk (`/var/repos/astra`) в файл `/etc/apt/sources.list.d/termidesk_local.list` через командный интерпретатор `sh`:

```
sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs) non-free" > /etc/apt/sources.list.d/termidesk_local.list'
```

где:

`-c` - ключ для чтения команд из вводимой строки (стандартный ввод);

`echo` - команда вывода текста, совместно с символом «>» используется для перенаправления строки `deb file:/var/repos/astra $(lsb_release -cs) non-free` в файл `/etc/apt/sources.list.d/termidesk_local.list`;

`deb file:/var/repos/astra $(lsb_release -cs) non-free` - добавляемый репозиторий, вложенная команда `$(lsb_release -cs)` подставляет версию - `1.7_x86-64`;

- выполнить поиск ключа репозитория Termidesk `GPG-KEY-PUBLIC` и добавить его в ОС:

```
cat /var/repos/astra/GPG-KEY-PUBLIC | sudo apt-key add -
```

- убедиться, что ключ `release@uveon.ru` был успешно добавлен:

```
apt-key list
```

В случае, если ключ не отображен в выводе команды, необходимо убедиться, что ключ `GPG-KEY-PUBLIC` существует:

```
cat /var/repos/astra/GPG-KEY-PUBLIC
```

Если ключ все же существует, необходимо проверить правильность выполнения шагов по добавлению репозитория Termidesk в файл `/etc/apt/sources.list.d/termidesk_local.list`.
При успешном выполнении всех шагов команда выведет содержимое ключа в формате Base64.

- обновить данные пакетного менеджера:

```
sudo apt update
```

Данную команду (`sudo apt update`) необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

2.2 . Установка STAL

Перед установкой необходимо подключить локальный репозиторий Termidesk, как указано в подразделе **Получение пакетов установки в ОС Astra Linux Special Edition**. ОС, на которую устанавливается STAL, должна быть установлена с графическим интерфейсом.

Для подключения к опубликованным приложениям и к терминальным сессиям можно использовать отдельные установки STAL для удобства разделения по функционалу: на одном сервере - только приложения, на другом - только терминальные сессии.

Начиная с оперативного обновления 1.7.5 ОС Astra Linux Special Edition 1.7 (бюллетень № 2023-1023SE17) улучшен механизм взаимодействия со STAL, поэтому для корректного функционирования STAL на ОС Astra Linux Special Edition 1.7.5 рекомендуется обновить ее до указанной в бюллетени версии (1.7.5.9).
В оперативном обновлении 1.7.6.UU.1 ОС Astra Linux Special Edition 1.7 (бюллетень № 2024-1108SE17MD) был обновлен пакет `fuse3`, поэтому для корректного функционирования STAL на ОС Astra Linux Special Edition 1.7.6 рекомендуется обновить ее до указанной в бюллетени версии (версии 1.7.6.14).
При наличии в файле `/etc/apt/sources.list` репозитория `astra-ce` нужно закомментировать его, чтобы избежать установки несовместимых версий пакетов.

Для корректной установки всех зависимостей в ОС Astra Linux Specail Edition в файле `/etc/apt/sources.list` должны быть указаны репозитории, соответствующие используемой и поддерживаемой Termidesk версии ОС.

Подробную информацию о сетевых репозиториях ОС Astra Linux Special Edition можно получить в справочном центре Astra Linux:

- для ОС Astra Linux Special Edition 1.8: https://wiki.astralinux.ru/pages/viewpage.action?pageId=302043111;
- для ОС Astra Linux Special Edition 1.7: https://wiki.astralinux.ru/pages/viewpage.action?pageId=158598882.

Например, для ОС Astra Linux Special Edition 1.7.5.9 файл будет следующим:

```
deb https://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.5/repository-base/ 1.7_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.5/repository-extended/ 1.7_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.5/repository-update/ 1.7_x86-64 main contrib non-free
```

Для установки STAL нужно воспользоваться командами:

```
sudo apt install stal-rdp-transport
sudo apt install stal
```

Установку можно также выполнить из deb-пакета, не подключая локальный репозиторий, командами:

```
sudo apt install /home/user/stal-rdp-transport_<версия>.deb
```

```
2 sudo apt install /home/user/stal_<версия>.deb
```

где:

/home/user/stal-rdp-transport_<версия>.deb - путь к deb-пакету поддержки протокола доставки для STAL (stal-rdp-transport);

/home/user/stal_<версия>.deb - путь к deb-пакету STAL.

После установки основных пакетов STAL нужно установить пакеты поддержки функциональности в следующей последовательности:

- stal-multimedia - пакет поддержки проигрывания звука;
- stal-redirect-api - пакет базового API, от которого зависят следующие пакеты;
- stal-redirect-drive - пакет реализации перенаправления диска;
- stal-redirect-print - пакет реализации перенаправления принтера;
- stal-redirect-clip - пакет реализации буфера обмена;
- stal-redirect-scard - пакет реализации перенаправления смарт-карт.

Установка выполняется командой:

```
1 sudo apt install stal-multimedia stal-redirect-api stal-redirect-drive stal-
redirect-print stal-redirect-clip stal-redirect-scard
```

> ⚠ После установки STAL нужно установить и настроить компонент «Сессионный агент» (termidesk-session-agent) из состава Termidesk.
> При использовании STAL в домене нужно задать параметру USE_USER_PRINCIPAL_NAME конфигурационного файла «Сессионного агента» значение «True», см. подраздел **Конфигурационный файл сессионного Агента** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент». Это позволит добавлять суффикс домена в передаваемые параметры при подключении к STAL.

Список зависимостей пакетов для ОС Astra Linux Special Edition 1.8 приведен в таблице (см. Таблица 1).

Таблица 1 – Список зависимостей пакетов

Пакет	Зависимости
stal	gawk, libstdc++6, libssl3, qtvirtualkeyboard-plugin, libqt5network5, libqt5widgets5, libqt5gui5, libmhash2, libjsoncpp25, libblkid1, libdbus-1-3, libdbus-c++-1-0v5, libx11-xcb1, libxcb-randr0, libxcb-cursor0, xserver-xorg-video-dummy, x11-xserver-utils, x11-xkb-utils, stal-rdp-transport, keyutils, dbus-x11, xterm
stal-rdp-transport	libxkbfile1, libdbus-1-3, libx11-6, libssl3, libkrb5-3, libicu72, libxfixes3, libxshmfence1, libxext6, libkeyutils1, libcairo2, libswscale6, libavcodec59, libavcodec-extra59, libmagickcore-6.q16-6, libmagickwand-6.q16-6
stal-redirect-api	libdbus-1-3, libdbus-c++-1-0v5

Пакет	Зависимости
stal-redirect-drive	libdbus-1-3, libdbus-c++-1-0v5, libfuse3-3, fuse3, stal-redirect-api
stal-redirect-print	libdbus-1-3, libdbus-c++-1-0v5, libjsoncpp25, libcups2, cups-daemon, cups-client, stal-redirect-api
stal-redirect-clip	libdbus-1-3, libdbus-c++-1-0v5, libfuse3-3, fuse3, stal-redirect-api
stal-multimedia	libdbus-1-3, libdbus-c++-1-0v5, libpulse0, pipewire-pulse, libopus0, libfaac0, libgsm1
stal-redirect-scard	libdbus-1-3, libdbus-c++-1-0v5, libpcsclite1, stal-redirect-api

После установки службы STAL автоматически добавляются в автозагрузку и запускаются.

Вручную выполнить перезапуск служб можно командой:

```
:~$ sudo systemctl restart termidesk-stal stal-proxy stal-rdpepc stal-watchdog
```

Проверка состояния STAL производится командами:

```
1 sudo systemctl status stal-proxy
2 sudo systemctl status termidesk-stal
3 sudo systemctl status stal-rdpepc
4 sudo systemctl status stal-watchdog
```

Строка «Active» отображает состояние сервиса, где статус «active (running)» означает успешный запуск.

> ⚠ Перед началом использования STAL доменными пользователями стоит убедиться в корректной настройке доменного сервера. Например, авторизоваться доменным пользователем в ОС по протоколу SSH или войти через интерфейс GNOME.

2.3 . Установка в режиме замкнутой программной среды

Замкнутая программная среда (ЗПС) является средством повышения безопасности ОС путем контроля целостности (неизменности) файлов. Механизм контроля реализован в виде невыгружаемого модуля ядра ОС Astra Linux Special Edition (модуль digsig_verif), выполняющего проверку электронной цифровой подписи файлов (ЭЦП).

Перед установкой компонента Termidesk необходимо установить пакет termidesk-digsig-keys, выполнив следующее:

- подключить репозиторий Termidesk или получить отдельный пакет termidesk-digsig-keys из репозитория;
- выполнить установку с использованием репозитория:

```
sudo apt -y install termidesk-digsig-keys
```

- либо выполнить установку из deb-пакета:

```
sudo apt install -y /home/user/termidesk-digsig-keys-XXXXXX_amd64.deb
```

где:

`-y` - ключ для пропуска подтверждения установки;

`/home/user/termidesk-digsig-keys-XXXXXX_amd64.deb` - расположение пакета `termidesk-digsig-keys-XXXXXX_amd64.deb`.

- перезагрузить ОС:

```
sudo reboot
```

- выполнить установку компонента Termidesk.

Для ЗПС может быть выполнена активация режима проверки встроенной ЭЦП в расширенных атрибутах (`DIGSIG_XATTR_MODE`). В этом случае потребуется подписать файлы, которые будут проходить проверку, на имеющихся в организации ключах. Информация о процессе подписи и активации механизма проверки встроенной ЭЦП в расширенных атрибутах приведена в справочном центре Astra Linux: https://wiki.astralinux.ru/pages/viewpage.action?pageId=41190634.

2.4 . Удаление STAL

Удаление STAL выполняется командой:

```
sudo aptitude purge -y stal stal-multimedia stal-redirect-api stal-redirect-drive stal-redirect-print stal-redirect-clip stal-redirect-scard
```

где:

`-y` - ключ для пропуска подтверждения удаления.

После удаления необходимо очистить оставшиеся зависимости и конфигурации:

```
sudo aptitude purge ~c -y
```

Команда полностью удалит оставшиеся настройки и зависимости уже удаленных пакетов.

2.5 . Обновление STAL

Обновление STAL выполняется установкой новой версии поверх предыдущей.

> В релизе Termidesk версии 5.1 совместимость «Сессионного агента» со STAL предыдущих версий не поддерживается. При обновлении STAL на новую версию нужно обновить и «Сессионный агент» на новую версию, выпущенную в релизе.

2.6 . Постановка STAL на контроль целостности

После установки и настройки STAL необходимо поставить его на контроль целостности.

Для контроля целостности используются встроенные в ОС Astra Linux Special Edition программные средства на основе `Another File Integrity Checker`, представленного пакетом `afick`.

Настройка регламентного контроля целостности выполняется в конфигурационном файле `/etc/afick.conf`.

> Настройку следует производить только после окончательного внедрения компонента, поскольку с файлов конфигурации и исполняемых файлов будут сняты эталонные контрольные суммы.

Для постановки на контроль целостности STAL необходимо добавить в конфигурационный файл `/etc/afick.conf` следующие строки:

> Перечень содержит список строк для компонента «Сессионный агент», поскольку он ставится совместно со STAL.

```
/etc/dbus-1/session.d/ru.uveon.stal.multimedia.conf PARSEC
/etc/dbus-1/session.d/ru.uveon.stal.rdpdr.conf PARSEC
/etc/dbus-1/system.d/ru.uveon.stal.conf PARSEC
/etc/dbus-1/system.d/ru.uveon.stal.rdpepc.conf PARSEC
/etc/syslog-ng/conf.d/stal-clip.conf PARSEC
/etc/syslog-ng/conf.d/stal-fuse.conf PARSEC
/etc/syslog-ng/conf.d/stal-multimedia.conf PARSEC
/etc/syslog-ng/conf.d/stal-proxy.conf PARSEC
/etc/syslog-ng/conf.d/stal-rdpdr.conf PARSEC
/etc/syslog-ng/conf.d/stal-rdpepc.conf PARSEC
/etc/syslog-ng/conf.d/stal-scard.conf PARSEC
/etc/syslog-ng/conf.d/stal-service.conf PARSEC
/etc/syslog-ng/conf.d/stal-watchdog.conf PARSEC
/etc/systemd/system/multi-user.target.wants/stal-rdpepc.service PARSEC
/usr/lib/systemd/system/stal-proxy.service PARSEC
/usr/lib/systemd/system/stal-rdpepc.service PARSEC
/usr/lib/systemd/system/stal-watchdog.service PARSEC
/usr/lib/systemd/system/termidesk-stal.service PARSEC
/usr/share/dbus-1/services/ru.uveon.stal.multimedia.service PARSEC
/usr/share/dbus-1/services/ru.uveon.stal.rdpdr.service PARSEC
/var/lib/stal PARSEC
/var/lib/stal-proxy PARSEC
/var/spool/stal PARSEC
/etc/systemd/system/multi-user.target.wants/termidesk-stal.service PARSEC
/etc/systemd/system/termidesk-stal.service PARSEC
/etc/X11/Xresources/x11-stal PARSEC
/etc/X11/stal.conf PARSEC
/etc/dbus-1/system.d/ru.uveon.stal.conf PARSEC
/etc/logrotate.d/stal PARSEC
/etc/pam.d/stal PARSEC
```

```
/etc/pam.d/stal-rdp PARSEC
/etc/stal PARSEC
/etc/syslog-ng/conf.d/stal-proxy.conf PARSEC
/etc/syslog-ng/conf.d/stal-service.conf PARSEC
/etc/syslog-ng/conf.d/stal-watchdog.conf PARSEC
/etc/systemd/system/multi-user.target.wants/stal-proxy.service PARSEC
/etc/systemd/system/multi-user.target.wants/stal-watchdog.service PARSEC
/etc/systemd/system/multi-user.target.wants/termidesk-stal.service PARSEC
/etc/systemd/system/stal-proxy.service PARSEC
/etc/systemd/system/stal-watchdog.service PARSEC
/etc/systemd/system/termidesk-stal.service PARSEC
/etc/ufw/applications.d/stal-proxy PARSEC
/usr/libexec/stal PARSEC
/usr/sbin/stal_proxy PARSEC
/usr/sbin/stal_service PARSEC
/usr/sbin/stal_watchdog PARSEC
/usr/share/doc/stal PARSEC


#Репозиторий Termidesk
/var/repos/ PARSEC
```

Для снятия эталонных значений контрольных сумм используется команда:

```
afick -i
```

Для проверки соответствия контрольных сумм эталонным значениям автоматически создаются задания в системном планировщике заданий `cron`.

Для ручной проверки соответствия контрольных сумм используется команда:

```
afick -k
```

> ⚠ В случае отсутствия по какой-либо причине исполняемых фалов `*.pyc`, они будут повторно сгенерированы при перезапуске сервера Python. В этом случае нужно повторно проинициализировать средство регламентного контроля целостности `afick`.

3 . НАСТРОЙКА КОМПОНЕНТА

3.1 . Параметры конфигурирования STAL

Для настройки STAL используются конфигурационные файлы `/etc/stal/stal_service.json`, `/etc/stal/stal_proxy.json` и `/etc/stal/stal_kiosk.json`.

> ⚠ В большинстве случаев STAL не требует изменения конфигурационных файлов после установки. Описание файлов приведено для расширенной настройки.

Параметры внутри конфигурационных файлов имеют следующую структуру:

```
{
    "параметр": "значение",
    "параметр": [ "значение 1", ..., "значение N" ],
    "параметр": [ "значение 1", "%{значение 2}", ..., "значение N" ],
    "параметр": [ "аргумент:%{значение}" ]
}
```

Поля `%{значение}` используются для подстановки служебных значений.

> ⚠ Целочисленные значения не заключаются в кавычки.

Файл `/etc/stal/stal_proxy.json` определяет параметры работы сервиса `stal-proxy`, обеспечивающего передачу трафика от клиентских соединений на локальный сокет. Пример файла `/etc/stal/stal_proxy.json`:

```
{
    "debug:level": "debug",
    "transport:debug": false,
    "transport:shm": true,
    "transport:fps": 5,

    "listen:port": 3389,
    "listen:addr": "0.0.0.0",
    "listen:timeout": 10,

    "#kerberos:realm": "UVEON",
    "#kerberos:keytab": "/etc/stal/termsrv.keytab",

    "#x11rdp:path": "/usr/libexec/stal/freerdp-shadow-cli",
    "x11rdp:args": [ "/ipc-socket:%{socket}", "/max-connections:1", "-gfx-rfx", "+gfx-progressive", "-gfx-planar", "-gfx-avc420", "-gfx-avc444" ],
    "#tcp:keepalive:enable": true,
    "tcp:keepalive:delay": 5,
    "tcp:keepalive:retries": 3,
    "tcp:keepalive:interval": 2
}
```

Список доступных параметров конфигурационного файла `/etc/stal/stal_proxy.json` приведен в таблице (см. Таблица 2).

Таблица 2 – Описание параметров файла конфигурации сервиса proxy

Параметр	Назначение	Значение по умолчанию
`debug:level`	Уровень отладочных сообщений. Возможные значения: `debug`, `info`, none	`debug`
`transport:debug`	Управление режимом отладочного журналирования для протокола RDP (`freerdp-shadow`). По умолчанию режим отладочного журналирования выключен. Для включения необходимо присвоить параметру значение `true`	`false`
`transport:shm`	Управление механизмом совместного доступа к памяти. Механизм позволяет передавать видеоизображение через общую память для сокращения задержки и снижения нагрузки на сеть. Возможные значения: ▪ `true` - использовать механизм совместного доступа к памяти; ▪ `false` - не использовать механизм совместного доступа к памяти	`true`
`transport:fps`	Управление частотой передачи кадров в секунду. Параметр влияет на соотношение качества видеоизображения и нагрузки на сервер. Увеличение значения улучшает плавность видеоизображения, но требует больших ресурсов процессора. Уменьшение значения снижает нагрузку на процессор, но ухудшает плавность видеоизображения. Диапазон значений: от 5 до 25	`5`
`listen:port`	Сервисный порт доступа	`3389`
`listen:addr`	Сетевой интерфейс для соединения	`0.0.0.0`
`listen:timeout`	Время ожидания клиентского подключения, в секундах	`10`
`kerberos:realm`	Домен `Kerberos`	`UVEON`
`kerberos:keytab`	Указание `keytab`-файла для аутентификации `Kerberos` для учетной записи сервера STAL. Файл `termsrv.keytab` после установки не существует, его необходимо создать на контроллере домена и скопировать в `/etc/stal/`	`/etc/stal/termsrv.keytab`
`x11rdp:path`	Системная программа запуска протокола RDP (поставляется с пакетом `freerdp`)	`/usr/libexec/stal/freerdp-shadow-cli`

Параметр	Назначение	Значение по умолчанию
x11rdp:args	Список аргументов для команды протокола RDP. Для получения краткой информации по доступным аргументам протокола RDP нужно воспользоваться командой: `/usr/libexec/stal/freerdp-shadow-cli /help` Для выбора кодеков, которые будут использоваться при декодировании видеоизображения нужно: ▪ указать знак «-» перед параметром для отключения кодека (например, "-gfx-rfx"); ▪ указать знак «+» перед параметром для включения кодека (например, "+gfx-rfx")	"/ipc-socket:%{socket}", "/max-connections:1", "-gfx-rfx", "+gfx-progressive", "-gfx-planar", "-gfx-avc420", "-gfx-avc444"
tcp:keepalive:enable	Управление механизмом keepalive по протоколу TCP. Механизм keepalive помогает разорвать зависшее соединение с минимальным временем ожидания. Возможные значения: ▪ false - подключение к сессии после разрыва соединения и его восстановления возможно только по прошествии некоторого времени; ▪ true - подключение к сессии после разрыва соединения возможно сразу после его восстановления	true
tcp:keepalive:delay	Время (в секундах) простоя соединения, по прошествии которого рольлелд TCP начнет отправлять проверочные пакеты	5
tcp:keepalive:retries	Максимальное число проверок протокола TCP, отправляемых перед сбросом соединения	3
tcp:keepalive:interval	Время (в секундах) между отправками отдельных проверочных пакетов	2

⚠ Некоторые параметры в JSON-файлах закомментированы - перед ними есть символ «#». Это значит, что такой параметр используется со значением по умолчанию. Чтобы его изменить, нужно удалить символ «#» и присвоить нужное значение параметру.
Пример:
по умолчанию в качестве домена Kerberos в параметре kerberos:realm файла /etc/stal/stal_proxy.json указан UVEON. Чтобы указать другой домен, например, example.local, нужно преобразовать параметр "#kerberos:realm": "UVEON" к "kerberos:realm": "example.local".

Файл /etc/stal/stal_service.json определяет параметры работы основного сервиса stal, обеспечивающего запуск и останов графических сессий пользователя и реализующего основной функционал STAL. Пример файла /etc/stal/stal_service.json:

```
{
    "debug:level": "debug",

    "#runtime:dir": "/run/stal",
```

```
    "#runtime:xdg": "/run/user/%{uid}",

    "#xvfb:path": "/usr/bin/Xorg",
    "#xvfb:args": [ ":%{display}", "-nolisten", "tcp", "-logfile", "/dev/null",
"-auth", "%{authfile}", "-config", "stal.conf", "-depth", "%{depth}",
"+extension", "DAMAGE", "+extension", "MIT-SHM", "+extension", "RANDR",
"+extension", "XFIXES", "+extension", "XTEST" ],
    "#xvfb:sock": "/tmp/.X11-unix/X%{display}",

    "#pam:service": "stal",

    "users:limit": 200,
    "sessions:limit": 1000,

    "#groups:allow": [],

    "session:path": "/usr/bin/fly-wm",
    "session:args": [ ],
    "session:programs": "/etc/stal/programs.json",

    "start:timeout": 15,
    "#seamless:timeout": 60,
    "#inactivity:timeout": 0,
    "#duration:timeout": 0,
    "#disconnect:timeout": 0,
    "#clipboard:limit": 0,

    "#redirect:drive": true,
    "#redirect:print": true,
    "#redirect:smartcard": true,
    "#clipboard:file": true,
    "#clipboard:server": true,
    "#clipboard:client": true,

    "#connect:policy": "PrevReplace",
    "#session:disconnected:freeze": false,
    "#login:helper": false,
    "#login:sessions": false,
    "#login:keyboard": false,

    "#rdp:keepalive:interval": 0,
    "#rdp:keepalive:failures": 0,

    "applications:skip": [ "1cestart.desktop" ],

    "#helper:notification": "/usr/libexec/stal/stal_notify",
    "#xrandr:path": "/usr/bin/xrandr",

    "#tdsk:enable": false,
    "#tdsk:fstype": "ext4",
    "#tdsk:option": ""
}
```

Список доступных параметров конфигурационного файла `/etc/stal/stal_service.json` приведен в таблице (см. Таблица 3).

Таблица 3 – Описание параметров файла конфигурации сервиса STAL

Параметр	Назначение	Значение по умолчанию
`debug:level`	Уровень отладочных сообщений. Возможные значения: `debug`, `info`, `none`	`debug`
`runtime:dir`	Рабочий каталог сервиса STAL	`/run/stal`
`runtime:xdg`	XDG-каталог сессии	`/run/user/%{uid}`
`xvfb:path`	Путь запуска X11-сервера	`/usr/lib/xorg/Xorg`
`xvfb:args`	Список аргументов X11-сервера. Возможны подстановки служебных значений: `%{display}`, `%{authfile}`, `%{depth}`, `%{width}`, `%{height}`	Приведено в примере `/etc/stal/stal_service.json`
`xvfb:sock`	Формат сокета для X11-сервера. Возможна подстановка служебного значения: `%{display}`	`/tmp/.X11-unix/X%{display}`
`pam:service`	Идентификатор сервиса доступа `PAM`	`stal`
`users:limit`	Ограничение на количество пользователей, подключившихся к STAL	`200`
`sessions:limit`	Ограничение на количество сессий, запущенных на STAL	`1000`
`groups:allow`	Список разрешенных групп пользователей для аутентификации на сервере STAL. Если параметр закомментирован, то аутентификация разрешена всем пользователям, иначе только пользователям, которые состоят в перечисленных группах. Пример: `"groups:allow":["group1", "group2"]`	`[]`
`session:path`	Клиентская программа, запускаемая в сессии	`/usr/bin/fly-wm`
`session:args`	Список аргументов для запуска клиентской программы	`Не задано`
`session:programs`	Файл списка разрешенных программ для режима `seamless`, формат `json`	`/etc/stal/programs.json`
`start:timeout`	Таймаут (в секундах) запуска сессии	`15`
`seamless:timeout`	Таймаут жизни программной сессии (`seamless`) после отключения, в секундах	`60`
`inactivity:timeout`	Лимит бездействия пользовательской сессии по умолчанию, в секундах	`0`
`duration:timeout`	Лимит продолжительности работы пользовательской сессии по умолчанию, в секундах	`0`
`disconnect:timeout`	Таймаут жизни пользовательской сессии после отключения, в секундах	`0`

Параметр	Назначение	Значение по умолчанию
`clipboard:limit`	Максимальный лимит буфера обмена в байтах (0: не ограничено). Для блокировки буфера обмена нужно использовать параметры `clipboard:server` и `clipboard:client`	`0`
`redirect:drive`	Политика для перенаправления дисков/каталогов в RDP. По умолчанию включена	`true`
`redirect:print`	Политика для перенаправления принтеров в RDP. По умолчанию включена	`true`
`redirect:smartcard`	Политика для перенаправления смарт-карт в RDP. По умолчанию включена	`true`
`clipboard:file`	Политика для перенаправления файлов через буфер обмена на сервер. По умолчанию включена	`true`
`clipboard:server`	Политика для перенаправления буфера обмена на сервер. По умолчанию включена	`true`
`clipboard:client`	Политика для перенаправления буфера обмена на клиент. По умолчанию включена	`true`
`connect:policy`	Политика для множественного соединения в сессию. Возможные значения: `NextDeny` (если сессия занята, следующее соединение в нее отменяется), `PrevReplace` (если сессия занята, предыдущее соединение в нее отменяется), `MultiAllow` (разрешено множественное соединение)	`PrevReplace`
`session:disconnected:freeze`	Приостанов («заморозка») группы выполняемых процессов сессии при отсутствии подключений. Параметр предоставляет возможность сэкономить ресурсы процессора. Возможные значения: ▪ `false` - отключено; ▪ `true` - включено	`false`
`login:helper`	Поддержка графического диалога входа в ОС. Возможные значения: ▪ `false` - отключено; ▪ `true` - включено	`false`
`login:sessions`	Поддержка выбора сессии пользователя в графическом диалоге входа в ОС. Возможные значения: ▪ `false` - отключено; ▪ `true` - включено	`false`
`login:keyboard`	Поддержка виртуальной клавиатуры в графическом диалоге входа в ОС. Возможные значения: ▪ `false` - отключено; ▪ `true` - включено	`false`
`rdp:keepalive:interval`	Время в секундах между отправками отдельных проверочных пакетов для механизма `keepalive` по протоколу RDP	`0`
`rdp:keepalive:failures`	Максимальное число ошибок, допустимых перед сбросом соединения	`0`

Параметр	Назначение	Значение по умолчанию
`applications:skip`	Список запрещенных программ, которые не будут опубликованы. В значении параметра должен указываться ярлык программы: <имя программы>.desktop	`1cestart.desktop`
`helper:notification`	Служебная программа для информирования в сессии через механизм нотификаций (всплывающих сообщений)	`/usr/libexec/stal/stal_notify`
`xrandr:path`	Системная программа для изменения геометрии экрана в сессии	`/usr/bin/xrandr`
`tdsk:enable`	Служебный параметр. Менять не следует	`false`
`tdsk:fstype`	Служебный параметр. Менять не следует	`ext4`
`tdsk:option`	Служебный параметр. Менять не следует	`Не задано`

Файл `/etc/stal/stal_kiosk.json` определяет (см. Рисунок 1) свойства окон приложений, запускаемых в режиме доставки приложений (киоск).

ⓘ Функциональность режима приложений `stal_kiosk` поддерживается в ОС Astra Linux Special Edition только для уровня защищенности «Орел».

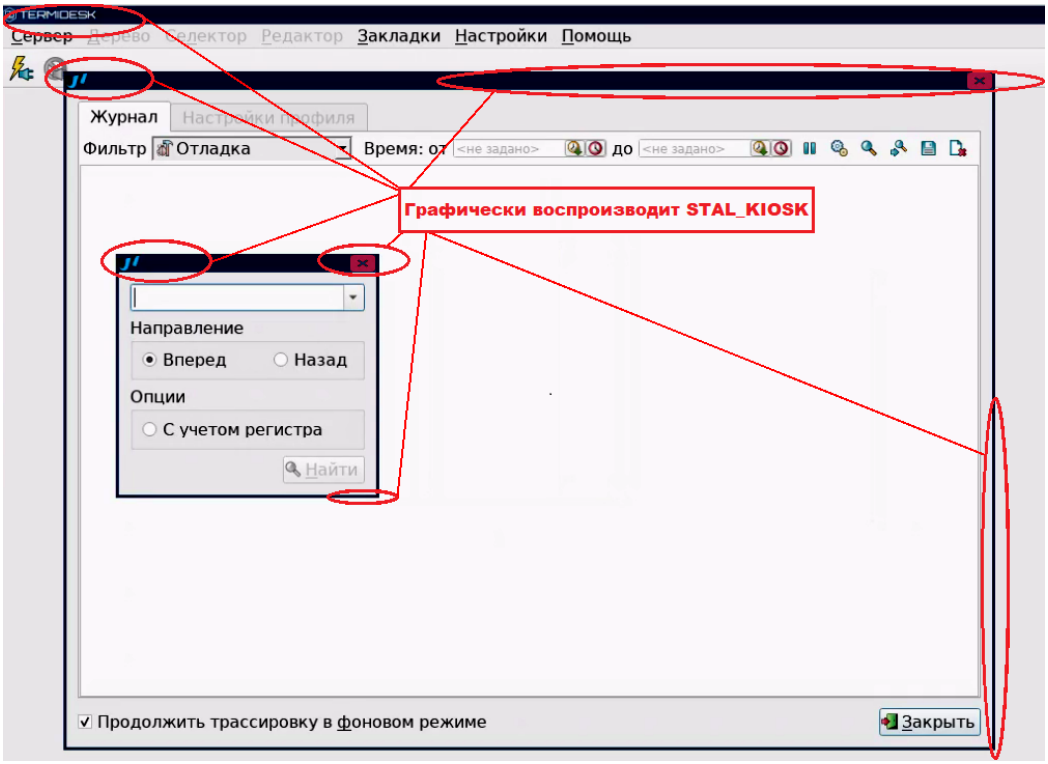

Рисунок 1 – Влияние stal_kiosk на поведение окна

Пример файла `/etc/stal/stal_kiosk.json`:

```
[
    {
        "wm:window:type": "dialog",
        "wm:class": "1cv8*",
        "wm:window:role": "GtkFileChooserDialog",
        "frame": false,
        "fullscreen": true
    },
    {
        "wm:window:type": "dialog",
        "wm:class": "1cv8*",
        "frame": false,
        "fullscreen": false
    },
    {
        "wm:class": "xterm",
        "frame": false,
        "fullscreen": true
    },
    {
        "wm:window:type": "normal",
        "wm:class": "*",
        "frame": false,
        "fullscreen": true
    },
    {
        "wm:window:type": "dialog",
```

```
        "wm:class": "*",
        "frame": true,
        "fullscreen": false
    }
]
```

Поведение окон, описанное в файле конфигурации `/etc/stal/stal_kiosk.json`, реализуется по тегам системной утилиты `xprop`. Список доступных параметров приведен в таблице (см. Таблица 4).

Для получения значения тега для определенного окна нужно:

- запустить окно нужного приложения;
- запустить утилиту `xprop` из интерфейса командной строки:

```
xprop
```

- выбрать левой кнопкой мыши открытое окно, теги которого необходимо получить;
- информация по тегам утилиты `xprop`, назначенных для этого окна, отобразится в интерфейсе командной строки, пример:

```
WM_NAME(COMPOUND_TEXT) = "Домашняя - Менеджер файлов"
_NET_WM_NAME(UTF8_STRING) = "Домашняя - Менеджер файлов"
_MOTIF_WM_HINTS(_MOTIF_WM_HINTS) = 0x3, 0x3e, 0x7e, 0x0, 0x0
_NET_WM_WINDOW_TYPE(ATOM) = _NET_WM_WINDOW_TYPE_NORMAL
_XEMBED_INFO(_XEMBED_INFO) = 0x0, 0x1
WM_CLIENT_LEADER(WINDOW): window id # 0x3200008
WM_HINTS(WM_HINTS):
                Client accepts input or input focus: True
                window id # of group leader: 0x3200008
WM_CLIENT_MACHINE(STRING) = "cl-00000"
_NET_WM_PID(CARDINAL) = 1721
_NET_WM_SYNC_REQUEST_COUNTER(CARDINAL) = 52429217
WM_CLASS(STRING) = "fly-fm-service", "fly-fm-service"
WM_PROTOCOLS(ATOM): protocols  WM_DELETE_WINDOW, WM_TAKE_FOCUS, _NET_WM_PING,
_NET_WM_SYNC_REQUEST
WM_NORMAL_HINTS(WM_SIZE_HINTS):
                user specified size: 1333 by 913
                program specified minimum size: 182 by 219
                window gravity: Static
```

Таблица 4 – Описание параметров файла конфигурации stal_kiosk

Параметр	Назначение
`wm:window:type`	Соответствует тегу `_NET_WM_WINDOW_TYPE` утилиты `xprop`. Допустимые значения: «dialog», «utility», «splash», «menu», «popup_menu», «tooltip», «notification», «normal»
`wm:class`	Соответствует тегу `WM_CLASS` утилиты `xprop`
`wm:window:role`	Соответствует тегу `WM_WINDOW_ROLE` утилиты `xprop`
`frame`	Определяет реализуемое действие: использовать (`true`) или запретить (`false`) дополнительное оформление окна

Параметр	Назначение
`fullscreen`	Определяет реализуемое действие: использовать (`true`) или запретить (`false`) полноэкранный режим для окна

Главное окно приложения всегда запускается в полноэкранном режиме!

3.2 . Настройка динамического разрешения экрана и поддержки высокого разрешения

STAL поддерживает включение динамического разрешения экрана при подключении пользователя через компонент «Клиент» к терминальной сессии или опубликованному в STAL приложению.

Для того, чтобы включить динамическое разрешение, нужно:

- в «Портале администратора» перейти в «Компоненты - Протоколы доставки»;
- открыть настройки используемого для подключения протокола доставки (для STAL это протоколы «Доступ к STAL по RDP (напрямую) [экспериментальный]» или «Доступ к STAL по RDP (через шлюз) [экспериментальный]»);
- переключить параметр «Динамическое разрешение» в значение «Да»;
- нажать кнопку **[Сохранить]**.

В случае, если пользователь подключается к терминальной сессии STAL или получает опубликованное приложение с ОС Microsoft Windows 11, функциональность динамического разрешения экрана не работает и данный параметр должен быть переведен в значение «Нет».

Динамическое разрешение поддерживается в STAL, начиная с версии 1.0, в компоненте «Универсальный диспетчер» версии 4.2 и выше, в компоненте «Клиент» с версии 4.2.

Также рекомендуется включить сглаживание шрифтов перед первым входом пользователя в терминальную сессию, для этого:

- на сервере STAL перейти «Звезда - Панель управления - Рабочий стол - Шрифты»;
- задать параметру «Сглаживание» значение «Включить» и нажать кнопку [Применить] (см. Рисунок 2).

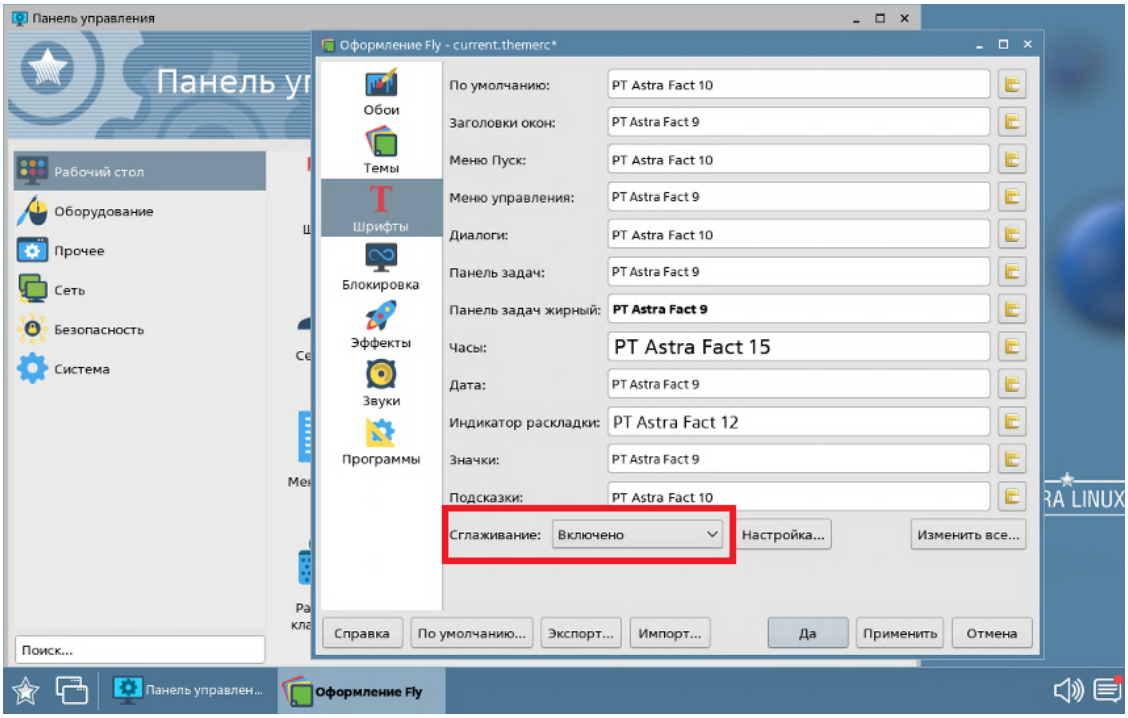

Рисунок 2 – Включение сглаживания шрифтов

При необходимости поддержки экранов высокого разрешения необходимо на сервере STAL отредактировать файл `/etc/X11/stal.conf`, раскомментировав нужный режим (режимы) в блоке строк `Modeline`:

```
Modeline "8192x4096"  252.50  8192 8400 9216 10240  4096 4099 4109 4113 -hsync +vsync
Modeline "5496x1200"  257.25  5496 5696 6256 7016  1200 1203 1213 1224 -hsync +vsync
Modeline "5280x1080"  262.00  5280 5496 6032 6784  1080 1083 1093 1105 -hsync +vsync
Modeline "5280x1200"  284.75  5280 5512 6056 6832  1200 1203 1213 1226 -hsync +vsync
Modeline "5120x3200"  277.75  5120 5344 5872 6624  3200 3203 3209 3227 -hsync +vsync
Modeline "4800x1200"  267.00  4800 5016 5512 6224  1200 1203 1213 1227 -hsync +vsync
Modeline "3840x2880"  297.50  3840 4072 4472 5104  2880 2883 2887 2916 -hsync +vsync
Modeline "3840x2560"  262.00  3840 4048 4448 5056  2560 2563 2573 2592 -hsync +vsync
Modeline "3840x2048"  262.75  3840 4048 4448 5056  2048 2051 2061 2080 -hsync +vsync
Modeline "3840x1080"  283.25  3840 4064 4464 5088  1080 1083 1093 1114 -hsync +vsync
Modeline "3600x1200"  296.75  3600 3824 4200 4800  1200 1203 1213 1238 -hsync +vsync
Modeline "3440x1440"  270.00  3440 3648 4008 4576  1440 1443 1453 1476 -hsync +vsync
Modeline "3288x1080"  296.00  3288 3504 3848 4408  1080 1083 1093 1120 -hsync +vsync
```

```
Modeline "2048x2048"  295.25  2048 2208 2424 2800  2048 2051 2061 2109 -hsync +vsync
Modeline "2048x1536"  267.25  2048 2208 2424 2800  1536 1539 1543 1592 -hsync +vsync
Modeline "2560x1600"  286.00  2560 2744 3016 3472  1600 1603 1609 1649 -hsync +vsync
Modeline "2560x1440"  256.25  2560 2736 3008 3456  1440 1443 1448 1484 -hsync +vsync
Modeline "1920x1440"  233.50  1920 2064 2264 2608  1440 1443 1447 1493 -hsync +vsync
Modeline "1920x1200"  193.25  1920 2056 2256 2592  1200 1203 1209 1245 -hsync +vsync
Modeline "1920x1080"  173.00  1920 2048 2248 2576  1080 1083 1088 1120 -hsync +vsync
Modeline "1680x1050"  146.25  1680 1784 1960 2240  1050 1053 1059 1089 -hsync +vsync
Modeline "1600x1200"  161.00  1600 1712 1880 2160  1200 1203 1207 1245 -hsync +vsync
Modeline "1600x900"  118.25  1600 1696 1856 2112  900 903 908 934 -hsync +vsync
Modeline "1440x900"  106.50  1440 1528 1672 1904  900 903 909 934 -hsync +vsync
Modeline "1368x768"   85.25  1368 1440 1576 1784  768 771 781 798 -hsync +vsync
Modeline "1280x1024"  109.00  1280 1368 1496 1712  1024 1027 1034 1063 -hsync +vsync
Modeline "1360x768"   84.75  1360 1432 1568 1776  768 771 781 798 -hsync +vsync
Modeline "1280x800"   83.50  1280 1352 1480 1680  800 803 809 831 -hsync +vsync
Modeline "1280x768"   79.50  1280 1344 1472 1664  768 771 781 798 -hsync +vsync
Modeline "1024x768"   63.50  1024 1072 1176 1328  768 771 775 798 -hsync +vsync
```

После сохранения файла перезапускать службы `stal` не нужно. Внесенные изменения будут активированы для новых сессий.

3.3 . Задание списка разрешенных программ

Список разрешенных программ создается двумя механизмами, дополняющими друг друга:

- автоматически, через сканирование каталога `/usr/share/applications` файлов `desktop`;
- вручную, дополнительно файлом `/etc/stal/programs.json`.

По умолчанию в файле `/etc/stal/programs.json` задается список дополнительных программ, которые не создавали файл `desktop` в системном каталоге `/usr/share/applications`. Для включения сканирования списка программ нужно установить значение параметра `session:programs` в конфигурационном файле `/etc/stal/stal_service.json`.

Параметры внутри файла `/etc/stal/programs.json` имеют следующую структуру:

```
[
    {
        "name": "наименование приложения",
        "path": "путь для запуска приложения" ,
        "args": [ "аргумент запуска 1", ..., "аргумент запуска N" ],
    }
]
```

Пример файла:

```
[
    {
        "name": "Midnight Commander",
        "path": "/usr/bin/xterm",
        "args": [ "-e", "/usr/bin/mc" ]
    },
    {
        "name": "Chromium Gost",
        "path": "/usr/bin/chromium-gost",
        "args": []
    }
]
```

Консольные программы необходимо запускать через графический терминал (см. пример для `Midnight Commander`).

> ⚠ Несистемные программы, требующие дополнительных настроек переменных среды, например `LD_LIBRARY_PATH`, следует запускать отдельным файлом сценария (скриптом), в котором все эти переменные должны быть определены.

Пример файла сценария для определения переменных среды и запуска программы `RuBackup Manager`:

```
#!/bin/bash
export PATH=$PATH:/opt/rubackup/bin
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/rubackup/lib

/opt/rubackup/bin/rbm

exit 0
```

3.4 . Задание списка запрещенных программ

В некоторых случаях может потребоваться задать список запрещенных программ, которые не должны быть опубликованы сервером STAL.

Такая необходимость может возникнуть в случае, если программа может выполняться в фоновом режиме. Например, в списке программ после установки 1С есть три исполняемых экземпляра:

- `1C:Enterprise x64`;
- `1C:Enterprise - Thin client x64`;
- `1C:Enterprise x64` - этот экземпляр запускает подпрограмму `1cestart`, которая выполняется только в фоновом режиме.

Список запрещенных программ задается через параметр `applications:skip` конфигурационного файла `/etc/stal/stal_service.json`. По умолчанию в нем уже хранится значение для запрета программы из приведенного выше примера - `1cestart.desktop`.

3.5 . Выполнение исполняемых файлов при подключении или отключении пользователя

Начиная со STAL версии 2.0 добавлена поддержка выполнения внешних исполняемых файлов, определенных администратором, при:

- подключении пользователя в сессию;
- отключении пользователя от сессии;
- запуске сессии пользователя;
- закрытии (останове) сессии пользователя.

Для мониторинга перечисленных выше событий существует служба `stal-watchdog`, запускаемая сразу после установки STAL.
Для выполнения внешних исполняемых файлов (например, `xx-scripts.sh`) администратору нужно:

- создать каталог `/etc/stal/sessions.d/`:

```
sudo mkdir /etc/stal/sessions.d/
```

- перейти в созданный каталог:

```
cd /etc/stal/sessions.d/
```

- создать в нем подкаталоги `created`, `connected`, `disconnected`, `closed`:

```
1 sudo mkdir created
2 sudo mkdir connected
3 sudo mkdir disconnected
4 sudo mkdir closed
```

- поместить нужные исполняемые файлы в соответствующие каталоги:
  - для выполнения при подключении пользователя в сессию - `/etc/stal/sessions.d/connected`;
  - для выполнения при отключении пользователя от сессии - `/etc/stal/sessions.d/disconnected`;
  - для выполнения при запуске сессии пользователя - `/etc/stal/sessions.d/created`;
  - для выполнения при закрытии (останове) сессии пользователя - `/etc/stal/sessions.d/closed`.

В исполняемых файлах можно использовать переменные среды, приведенные в таблице (см. Таблица 5).

Таблица 5 – Переменные среды, доступные для использования в исполняемых файлах

Переменная	Назначение
SESSION_LOGIN	Имя пользователя
SESSION_HOME	Рабочий каталог пользователя
SESSION_XAUTHFILE	Служебная переменная X11 сессии пользователя
SESSION_DISPLAY	Служебная переменная X11 сессии пользователя
SESSION_UID	Идентификатор пользователя
SESSION_GID	Идентификатор группы пользователя

SESSION_SYSTEMD_ID	Идентификатор сессии в системе управления службами systemd. Программный номер сессии STAL синхронизирован с номером сессии systemd.
	Для получения номера сессии можно выполнить команду:
	`:~$ sudo loginctl list-sessions`
	Для получения статуса сессии можно выполнить команду:
	`:~$ sudo loginctl session-status <номер сессии>`

SESSION_SEAMLESS	Режим seamless
SESSION_MOUNTED	Указывает, что профиль пользователя смонтирован
SESSION_COUNTS	Количество программных сессий пользователя

3.6 . Ограничение ресурсов сессии

В STAL поддерживается задание ограничений на используемые ресурсы: память, процессор, количество процессов и задач, работа с сетью. Ограничения задаются в конфигурационном файле /etc/stal/limits.json, по умолчанию применяются настройки секции «default».

Пример конфигурационного файла после установки STAL:

```
{
    "default": {
        "cpu:weight": 0,
        "cpu:quota": 0,
        "memory:high": "",
        "memory:max": "",
        "task:max": 0,
        "network:deny": "",
        "network:allow": ""
    },

    "groups": [
        {
            "name": "test-admins",
            "cpu:weight": 0,
            "cpu:quota": 0,
            "memory:high": "",
```

```
            "memory:max": "",
            "task:max": 1024
        },
        {
            "name": "test-users",
            "cpu:weight": 0,
            "cpu:quota": 20,
            "memory:high": "2G",
            "memory:max": "3G",
            "task:max": 256
        }
    ],

    "users": [
        {
            "name": "vasyan",
            "cpu:weight": 0,
            "cpu:quota": 3,
            "memory:high": "1G",
            "memory:max": "2G",
            "task:max": 128,
            "network:deny": "any",
            "network:allow": "localhost"
        }
    ]
}
```

Конфигурационный файл содержит секции:

- «default»: задает ограничения по умолчанию;
- «groups»: задает ограничения пользователя, если он состоит в указанной группе;
- «users»: задает ограничения пользователя.

Список доступных параметров конфигурационного файла `/etc/stal/limits.json` приведен в таблице (см. Таблица 6).

> Подробную информацию по используемым значениям параметров системы управления службами `systemd` можно получить по ссылке: https://www.freedesktop.org/software/systemd/man/latest/systemd.resource-control.html.

Таблица 6 – Описание параметров файла конфигурации limits.json

Параметр	Назначение
`name`	Имя группы или пользователя, к которому будут применены ограничения
`cpu:weight`	Соответствует параметру «CPUWeight» в системе управления службами `systemd`. Разрешенные значения от 1 до 10000, по умолчанию `systemd` задает 100. Значение «0»: функциональность не используется.

Параметр	Назначение
`cpu:quota`	Соответствует параметру «CPUQuota» в системе управления службами `systemd`. Значение указывается в процентах на одно ядро процессора. Значение «0»: функциональность не используется
`memory:high`	Ограничение использования памяти выполняемыми процессами. Ограничение может быть превышено, если это неизбежно, но в таких случаях процессы сильно замедляются. Соответствует параметру «MemoryHigh» в системе управления службами `systemd`. Значение задается в байтах. Также могут быть использованы суффиксы: ▪ K - килобайт, например: 1K; ▪ M - мегабайт, например: 1M; ▪ G - гигабайт, например: 1G; ▪ T - терабайт, например: 1T. Значение не задано: параметр и функциональность не используются
`memory:max`	Абсолютное ограничение использования памяти выполняемыми процессами. Если ограничение превышается, будет вызвано системное средство устранения нехватки памяти. Соответствует параметру «MemoryMax» в системе управления службами `systemd`. Значения задаются аналогично параметру `memory:high`. Значение не задано: функциональность не используется
`task:max`	Максимальное количество задач, которые можно создать для сессии. Соответствует параметру «TasksMax» в системе управления службами `systemd`. Значение «0»: функциональность не используется
`network:deny`	Соответствует параметру «IPAddressDeny» в системе управления службами `systemd`. В качестве значений можно указывать: ▪ разделенный пробелами список IP-адресов, каждый из которых может иметь значение маски после символа «/», например: 192.0.2.1/24; ▪ символическое имя «any»: любой узел; ▪ символическое имя «localhost»: локальный узел; ▪ символическое имя «link-local»: все локальные IP-адреса; ▪ символическое имя «multicast»: все IP-адреса многоадресной рассылки. Значение не задано: функциональность не используется
`network:allow`	Соответствует параметру «IPAddressAllow» в системе управления службами `systemd`. Значения задаются аналогично параметру `network:deny`. Значение не задано: функциональность не используется

Для контроля значений ресурсов нужно воспользоваться командами:

```
sudo loginctl list-sessions
sudo systemctl show session-SID.scope
sudo systemctl show user-UID.slice
```

где:

`SID` - идентификатор сессии пользователя;

`UID` - идентификатор пользователя.

3.7 . Оптимизация работы FreeRDP3

В параметрах конфигурирования STAL доступен выбор видеокодека для улучшения производительности при передаче графически насыщенного контента (видео, 3D-графики и анимации). Настройка видеокодека позволяет оптимизировать передачу видеоизображения по протоколу FreeRDP3.

Для оптимизации передачи графических данных по протоколу FreeRDP3 нужно отредактировать файл `/etc/stal/stal_proxy.json` и присвоить соответствующие значения параметрам `transport:shm`, `transport:fps` и `x11rdp:args` согласно подразделу **Параметры конфигурирования STAL**.

3.8 . Настройка аутентификации OIDC

Для настройки аутентификации OIDC в STAL нужно задать дополнительные параметры в конфигурационном файле `/etc/sssd/sssd.conf`.

Для этого после ввода ОС Astra Linux Special Edition в домен выполнить:

- отредактировать файл `/etc/sssd/sssd.conf`, присвоив параметру `use_fully_qualified_names` значение `True`;
- перезапустить службу `sssd`:

```
sudo systemctl restart sssd
```

3.9 . Перенаправление ресурсов

3.9.1 . Общие сведения

В текущей версии STAL поддерживает:

- перенаправление дисков и каталогов;
- перенаправление принтеров;
- перенаправление буфера обмена (файлы, текст, картинки);
- перенаправление смарт-карт;
- перенаправление звука.

Не поддерживается копирование файлов через буфер обмена с сервера STAL в пользовательскую ОС Astra Linux Special Edition, если в ОС установлено приложение `xfreerdp` ниже версии 3.0.0.

Перенаправление ресурсов не работает:

- при подключении высокоуровневым пользователем - это блокируется защитными механизмами ОС Astra Linux Special Edition («Смоленск», «Воронеж»);
- при использовании в ОС Astra Linux Special Edition 1.8 («Смоленск», «Воронеж») механизма ЗПС.

Правила перенаправления ресурсов для терминальных сессий задаются политиками фонда в «Портале администратора» (см. подраздел **Политики фонда рабочих мест** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»).

3.9.2 . Перенаправление принтеров в сервер терминалов STAL

По умолчанию для принтеров используется драйвер raw, который отправляет на печать задание без дополнительного конвертирования (как есть).

⚠ Перенаправление принтеров для ОС Astra Linux Special Edition 1.8 доступно только при отключении механизма мандатного контроля целостности в ОС.

ⓘ Если принтер понимает Postscript (PS) или Page Description Language (PCL), или другой язык, то достаточно получить информацию об используемом драйвере, добавить ее в файл `/etc/stal/stal_rdpepc.json` и перезапустить сервис `stal-rdpepc.service`, как приведено ниже.

Настройка перенаправления принтеров в STAL будет отличаться в зависимости от ОС пользовательской рабочей станции:

- ОС на базе Linux: задание raw-формата отправится без изменения и будет распечатано клиентской программой через систему печати CUPS, настроенной на пользовательской рабочей станции в соответствии с документацией на ОС. Дополнительные настройки на STAL в этом случае выполнять не нужно;
- ОС Microsoft Windows: может потребоваться конвертирование задания печати, потому что не все принтеры способны распечатать файл без дополнительного преобразования в поддерживаемый ими формат. В этом случае:
  - если для принтера не существует драйвер под ОС на базе Linux, то достаточно добавить программный виртуальный принтер PDF/XPS на пользовательской рабочей станции и не выполнять дополнительную настройку STAL;
  - если для принтера существует драйвер под ОС на базе Linux, то администратору нужно выполнить настройку STAL, описание которой приведено ниже. Настройка заключается в формировании файла, ассоциирующего драйвер принтера с драйвером системы CUPS.

Для настройки печати нужно выполнить на сервере STAL:

- установить драйвер для системы печати CUPS (x86_64) в соответствии с инструкцией драйвера;
- получить информацию об используемом пользователем драйвере:
  - выполнить поиск по фразе «driverName» в журнале `/var/log/termidesk/stal_rdpdr.log` для получения имени драйвера:

```
sudo grep -F "driverName" /var/log/termidesk/stal_rdpdr.log
```

- или получить информацию об имени драйвера командой:

```
sudo journalctl -t stal_rdpdr | grep rdpdrPrinterCreate
```

- затем получить информацию о CUPS-драйвере:

```
sudo lpinfo -m | grep -i <имя>
```

```
Пример вывода:
brother-HL1200-cups-en.ppd Brother HL1200 for CUPS
lsb/usr/brother/brother-HL1200-cups-en.ppd Brother HL1200 for CUPS
```

⚠ Параметр `<имя>` следует задавать по наименованию производителя, а не имени драйвера, например, `brother`.

- создать файл `/etc/stal/stal_rdpepc.json` и добавить в него полученную информацию. Пример файла:

```
{
  "Brother HL-1200 series": "brother-HL1200-cups-en.ppd",
  "Brother HL-1500 series": "brother-HL1500-cups-en.ppd"
}
```

- перезапустить сервис `stal-rdpepc`:

```
sudo systemctl restart stal-rdpepc.service
```

После выполненной настройки при использовании пользователем принтера (в примере «Brother-1200») для печати будет использоваться ассоциация на нативный Linux-драйвер.

3.9.3 . Перенаправление дисков в STAL

Диски, отмеченные для перенаправления в сессию пользователя при подключении к STAL, монтируются в файловую систему ОС по пути `$XDG_RUNTIME_DIR/stal/$MOUNTPOINT`.

Обычно путь `$XDG_RUNTIME_DIR/stal/$MOUNTPOINT` соответствует `/run/user/<идентификатор_пользователя>/stal/<наименование_диска>`.

3.9.4 . Перенаправление смарт-карт в STAL

Для работы со смарт-картами в STAL нужно установить:

- драйверы и библиотеки, определенные производителем смарт-карт;
- ПО для работы со смарт-картами.

3.10 . Журналирование

STAL интегрирован с инструментом мониторинга событий и журналироваания auditd ОС Astra Linux Special Edition, а также с системой PAM. Применение настроенных параметров мониторинга событий осуществляется модулем pam_parsec_aud. По умолчанию регистрация событий включена в PAM-сценарии /etc/pam.d/stal.

Журналы работы STAL расположены в файлах /var/log/termidesk/stal_proxy.log, /var/log/termidesk/stal_rdpepc.log и /var/log/termidesk/stal_service.log при условии установленной в ОС службы ведения журналов syslog.

Параметры ротации журналов STAL определены конфигурационным файлом /etc/logrotate.d/stal.

В случае, если в ОС не установлена служба ведения журналов syslog, просмотр журналов выполняется командами:

```
sudo journalctl -t stal_proxy
sudo journalctl -t stal_service
sudo journalctl -t stal_rdpepc
sudo journalctl -t stal_watchdog
```

3.11 . Сбор журналов STAL

При возникновении нештатных ситуаций может понадобиться сбор всех журналов работы STAL и их отправка в техническую поддержку. Для удобства может использоваться исполняемый файл stalCreateReport.sh.

Для формирования файла архива с журналами нужно выполнить:

```
sudo /usr/libexec/stal/stalCreateReport.sh
```

В результате выполнения команды создастся файл /var/tmp/stal_report_YYYYMMDD_HHMI.tgz, где YYYY - год, MM - месяц, DD - день, HH - часы, MI - минуты формирования файла. При обращении в техническую поддержку необходимо приложить этот архив в запрос.

> ⚠ В случае, если какие-то из собираемых файлов журналов пусты, после выполнения команды может отобразиться ошибка «Нет такого файла или каталога», которая не влияет на формирование итогового файла архива.

4 . НЕШТАТНЫЕ СИТУАЦИИ

4.1 . Нештатные ситуации и способы их устранения

Возможные неисправности при работе со STAL и способы их устранения приведены в таблице (см. Таблица 7).

Таблица 7 – Перечень возможных нештатных ситуаций

Индикация	Описание	Возможное решение
Ошибка: «Ошибка сервера»	Ошибка появляется при попытке соединения к STAL	Ошибка появляется при установленном пакете `xserver-xorg-legacy` и связана со значением параметра `allowed_users` в файле `/etc/X11/Xwrapper.config`. Параметру необходимо присвоить значение `anybody`. Рекомендуемое решение: установить новейшую версию STAL
При добавлении поставщика ресурсов STAL или приложения в веб-интерфейсе Termidesk появляются ошибки «TypeError: 'NoneType' object is not iterable» и «Неверное имя пользователя и пароль»	Подключение к опубликованным приложениям перестало работать. Присутствует ошибка «The name ru.uveon.stal was not provided by any .service files» при запросе статуса службы `termidesk-session-agent`	Необходимо проверить журнал событий `/var/log/termidesk/stal_service.log` на наличие записей «Error from reader» и «Missing in array declaration». Наличие ошибок свидетельствует, что в файле `/etc/stal/programs.json` допущена синтаксическая ошибка. Рекомендуется также установить новейшую версию STAL
Отображается черное окно при подключении к терминальной сессии	Подключение к терминальной сессии не происходит, открывается черное окно и через секунду закрывается. Если пользователь еще не входил в ОС в графическом режиме, то в этом окне появляется надпись «Инициализация...», в домашнем каталоге пользователя создаются каталоги, но как только инициализация завершается, окно закрывается	Ошибка устранена в версии ОС Astra Linux Special Edition 1.7.5. Рекомендуется обновить ОС на версию ⩾ 1.7.5 и установить новейшую версию STAL
Не запускается опубликованное приложение	При подключении через STAL не происходит запуск опубликованных приложений. У подключившегося к STAL пользователя при этом может быть доступен рабочий стол и другие (неопубликованные) приложения	Необходимо проверить, установлен ли пакет `xrdp` на сервере STAL. Если он установлен, его необходимо удалить, поскольку `xrdp` занимает порт 3389, на котором работает STAL. Также возможна ситуация, когда некоторые программы не позволяют запускать другие свои копии. Поэтому необходимо проверить, было ли опубликованное приложение открыто в общей сессии того же пользователя, которая активна в данный момент. Если приложение было открыто, то нужно его закрыть и выйти (logout) из общей сессии. Для публикации некоторых из таких приложений можно использовать запуск с ключами, например `firefox --ProfileManager` или `chromium --temp-profile`

Индикация	Описание	Возможное решение
Нет подключения при попытке получить опубликованное приложение	При попытке получить опубликованное приложение возникает черный экран, подключения нет. STAL находится в домене MS AD	Необходимо проверить журнал событий `/var/log/termidesk/stal_service.log` на наличие записи «Permission denied». Наличие записи свидетельствует, что при вводе аутентификационных данных для подключения не был соблюден регистр букв в логине пользователя. Логин пользователя должен быть указан в точности такой, какой используется на доменном сервере
При попытке соединения к терминальному серверу или опубликованному на нем приложению соединение не устанавливается	При подключении к STAL соединение не устанавливается. При подключении к опубликованному приложению STAL вместо приложения отображается черный фон	Для устранения проблемы необходимо в «Портале администратора» Termidesk перейти «Рабочие места - Фонды», выбрать фонд STAL и задать ему значение политики «Механизм обеспечения безопасности на уровне сети (RDP)»: «TLS» или «RDP»
При попытке подключения возникает ошибка «Этот сеанс будет прекращен из-за ошибки протокола. Попробуйте подключиться заново к удаленному компьютеру»	Ошибка появляется при попытке соединения к STAL через стандартную утилиту Windows `mstsc`	Необходимо проверить значение политики «Политика управления глубиной цвета (RDP)» в «Портале администратора» компонента «Универсальный диспетчер»: значение политики должно быть «32 бит»
При запуске сессии воспроизводится звук, который к данной сессии не привязан	При подключении к STAL пользователю воспроизводится звук, который не был им запущен для проигрывания	Необходимо проверить наличие других активных сессий для данного пользователя (соединения могут быть закрыты), восстановить соединение и закрыть программы проигрывания звука, или завершить ненужные сессии (выполнить logout)
Невозможно подключиться доменным пользователем к терминальному серверу STAL	При попытке подключиться доменным пользователем к STAL соединение не устанавливается	Необходимо проверить значение параметра `use_fully_qualified_names` в конфигурационном файле SSSD-сервисов ОС `/etc/sssd/sssd.conf`. Если параметру задано значение `True`, то в конфигурационном файле «Сессионного агента» нужно присвоить значение `True` параметру `USE_USER_PRINCIPAL_NAME`

5 . ПРИНЯТЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин	Определение
Виртуальное рабочее место	Развернутая на ВМ ОС с установленным «Агентом виртуального рабочего места» и необходимым прикладным ПО. Подключение происходит через протоколы удаленного доступа
Рабочее место (РМ)	Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа. Под РМ подразумеваются как виртуальное рабочее место, так и терминальный доступ или доступ к опубликованным на терминальном сервере приложениям
Гостевая ОС	ОС, функционирующая на ВМ
Поставщик ресурсов	ОС, платформа виртуализации или терминальный сервер (MS RDS/STAL), предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов РМ
Протокол доставки	Поддерживаемый в Termidesk протокол удаленного доступа к РМ
Компонент «Сессионный агент»	Компонент Termidesk. Устанавливается на терминальный сервер (MS RDS/STAL), активирует возможность множественного доступа пользователей к удаленным рабочим столам и приложениям
Компонент «Универсальный диспетчер»	Компонент Termidesk. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им РМ и контроля доставки РМ. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-vdi.service`
Фонд РМ	Совокупность подготовленных РМ для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей
Компонент «Сервер терминалов Astra Linux»	Компонент Termidesk. Также: STAL. Обеспечивает подключение пользовательских рабочих станций к РМ с ОС Astra Linux Special Edition через сеанс удаленного терминала

6 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Пояснение
ВМ	Виртуальная машина
ЗПС	Замкнутая программная среда
ОС	Операционная система
ПО	Программное обеспечение
РМ	Рабочее место
ЭЦП	Электронная цифровая подпись
API	Application Programming Interface (интерфейс прикладного программирования)
CUPS	Common Unix Printing System (система печати Unix)
IP	Internet Protocol (межсетевой протокол)
JSON	JavaScript Object Notation (стандартный текстовый формат для структурированных данных)
MS AD	Microsoft Active Directory (службы каталогов Microsoft)
MS RDS	Microsoft Remote Desktop Services (службы удаленного рабочего стола Microsoft)
PAM	Pluggable Authentication Module (подключаемый модуль аутентификации)
PCL	Page Description Language (язык описания страниц)
PDF	Portable Document Format (открытый формат электронных документов)
PS	PostScript (язык программирования и описания графических документов)
RDP	Remote Desktop Protocol (протокол удаленного рабочего стола)
TCP	Transmission Control Protocol (протокол управления передачей)
TLS	Transport Layer Security (протокол защиты транспортного уровня)
SSSD	System Security Services Daemon (системная служба, управляющая доступом к удаленным каталогам и механизмам аутентификации)
STAL	Terminal Server Astra Linux (сервер терминалов Astra Linux)
XPS	XML Paper Specification (открытый графический формат фиксированной разметки на базе XML)

UVEON
Unified Virtualization
Experience, Opportunities, Now

119571, г. Москва, Ленинский проспект,
д. 119А, помещ. 9Н
https://termidesk.ru/
Телефон: +7 (495) 975-1-975

Общий e-mail: info@uveon.ru
Отдел продаж: sales@uveon.ru
Техническая поддержка: support@uveon.ru