



Вариант лицензирования «TermideskTerminal»

РУКОВОДСТВО АДМИНИСТРАТОРА

СЛЕТ.10001-02 90 06

Версия 5.0. Выпуск от мая 2024 (с исправлениями
от 28.06.2024)

**Настройка компонента «Сервер
терминалов»**

ОГЛАВЛЕНИЕ

1 .	ОБЩИЕ СВЕДЕНИЯ.....	4
1.1 .	О документе.....	4
1.2 .	Назначение компонента «Сервер терминалов».....	4
1.3 .	Требования к программному и аппаратному обеспечению	4
1.4 .	Типографские соглашения	5
2 .	УСТАНОВКА И УДАЛЕНИЕ КОМПОНЕНТА	6
2.1 .	Получение пакетов установки в ОС Astra Linux Special Edition	6
2.2 .	Установка STAL	7
2.3 .	Удаление STAL.....	10
2.4 .	Обновление STAL	10
3 .	НАСТРОЙКА КОМПОНЕНТА	11
3.1 .	Параметры конфигурирования STAL.....	11
3.2 .	Настройка динамического разрешения экрана и поддержки высокого разрешения.....	18
3.3 .	Задание списка разрешенных программ.....	20
3.4 .	Задание списка запрещенных программ.....	22
3.5 .	Выполнение исполняемых файлов при подключении или отключении пользователя	22
3.6 .	Ограничение ресурсов сессии	23
3.7 .	Перенаправление ресурсов	26
3.7.1 .	Общие сведения	26
3.7.2 .	Перенаправление принтеров в сервер терминалов STAL	26
3.7.3 .	Перенаправление дисков в STAL.....	28
3.7.4 .	Перенаправление смарт-карт в STAL.....	28
3.8 .	Журналирование	28
3.9 .	Сбор журналов STAL	29
4 .	НЕШТАТНЫЕ СИТУАЦИИ	30
4.1 .	Нештатные ситуации и способы их устранения	30

5.	ПРИНЯТЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	32
6.	ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	33

1 . ОБЩИЕ СВЕДЕНИЯ

1.1 . О документе

Настоящий документ является шестой 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.10001-02 90 02 «Руководство администратора. Настройка программного комплекса».

1.2 . Назначение компонента «Сервер терминалов»

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

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

STAL позволяет выполнять доставку как рабочего стола ВРМ 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 ВРМ параметру «Механизм обеспечения безопасности на уровне сети (RDP)» должно быть задано значение «TLS» или «RDP» (см. подраздел **Политики фонда ВРМ** документа СЛЕТ.10001-02 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). 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 программного обеспечения (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 выполнить следующее:

- 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:

```
1  :~$ 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 с uid «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.

В файле `/etc/apt/sources.list` должны быть включены следующие источники пакетов (репозитории) для корректной установки всех зависимостей в ОС:

```
1 deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-base/
  1.7_x86-64 main contrib non-free
2 deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/
  1.7_x86-64 main contrib non-free
```

⚠ Начиная с оперативного обновления 1.7.5 ОС Astra Linux Special Edition (бюллетень № 2023-1023SE17) улучшен механизм взаимодействия со STAL, поэтому для корректного функционирования STAL рекомендуется обновить ОС Astra Linux Special Edition.

При наличии в файле

`/etc/apt/sources.list` репозитория `astra-ce` нужно закомментировать его, чтобы избежать установки несовместимых версий пакетов:

```
1 # Расширенный репозиторий (компонент astra-ce)
2 #deb https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-
  extended/ 1.7_x86-64 astra-ce
```

Для установки STAL нужно воспользоваться командами:

```
1 :~$ sudo apt install stal-rdp-transport
2 :~$ sudo apt install stal
```

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

```
1 :~$ sudo apt install /home/user/stal-rdp-transport_XXX_alse17_amd64.deb
2 :~$ sudo apt install /home/user/stal_XXX_alse17amd64.deb
```

где:

`/home/user/stal-rdp-transport_XXX_alse17_amd64.deb` - путь к deb-пакету поддержки протокола доставки для STAL (`stal-rdp-transport`);

`/home/user/stal_XXX_alse17_amd64.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 компонент «Сессионный агент» (`termidesk-session-agent`) из состава Termidesk.

Список зависимостей пакетов приведен в таблице (см. Таблица 1).

Таблица 1 – Список зависимостей пакетов

Пакет	Зависимости
<code>stal</code>	<code>gawk, libmhash2, libjsoncpp1, libblkid1, libdbus-1-3, libdbus-c++-1-0v5, libx11-xcb1, libxcb-randr0, libxcb-cursor0, xserver-xorg-video-dummy, x11-xserver-utils, stal-rdp-transport (>= 3.3.0), keyutils, dbus-x11, xterm</code>
<code>stal-rdp-transport</code>	<code>libxkbfile1, libdbus-1-3, libx11-6, libssl1.1, libkrb5-3, libicu63, libxfixes3, libxext6, libkeyutils1, libcairo2, libswscale5, libavcodec58, libavcodec-extra58, libswresample3, libmagickcore-6.q16-6, libmagickwand-6.q16-6</code>
<code>stal-redirect-api</code>	<code>libdbus-1-3, libdbus-c++-1-0v5</code>
<code>stal-redirect-drive</code>	<code>libdbus-1-3, libdbus-c++-1-0v5, libfuse3-3, fuse3, stal-redirect-api (>= 2.0.b5)</code>
<code>stal-redirect-print</code>	<code>libdbus-1-3, libdbus-c++-1-0v5, libjsoncpp1, libcups2, cups-daemon, cups-client, stal-redirect-api (>= 2.0.b5)</code>
<code>stal-redirect-clip</code>	<code>libdbus-1-3, libdbus-c++-1-0v5, libfuse3-3, fuse3, stal-redirect-api (>= 2.0.b5)</code>
<code>stal-multimedia</code>	<code>libdbus-1-3, libdbus-c++-1-0v5, libpulse0, pulseaudio, libopus0, libfaac0, libgsm1</code>
<code>stal-redirect-scard</code>	<code>libdbus-1-3, libdbus-c++-1-0v5, libpcsclite1, stal-redirect-api (>= 2.0.b5)</code>

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.

2.3 . 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 командой:

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

Команда полностью удалит оставшиеся настройки и зависимости уже удаленных пакетов.

2.4 . Обновление STAL

Обновление STAL выполняется установкой новой версии поверх предыдущей.

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:

```

1  {
2      "параметр": "значение",
3      "параметр": [ "значение 1", ..., "значение N" ],
4      "параметр": [ "значение 1", "%{значение 2}", ..., "значение N" ],
5      "параметр": [ "аргумент:%{значение}" ]
6  }
```

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`:

```

1  {
2      "debug:level": "debug",
3      "transport:debug": false,
4
5      "listen:port": 3389,
6      "listen:addr": "0.0.0.0",
7      "listen:timeout": 10,
8
9      "#kerberos:realm": "UVEON",
10     "#kerberos:keytab": "/etc/stal/termsrv.keytab",
11
12     "#x11rdp:path": "/usr/libexec/stal/freerdp-shadow-cli",
13     "#x11rdp:args": [ "/ipc-socket:%{socket}", "/max-connections:1" ],
14     "#tcp:keepalive:enable": true,
15     "tcp:keepalive:delay": 5,
16     "tcp:keepalive:retries": 3,
17     "tcp:keepalive:interval": 2
18 }
```

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

Таблица 2 – Описание параметров файла конфигурации сервиса проху

Параметр	Назначение	Значение по умолчанию
debug:level	Уровень отладочных сообщений. Возможные значения: debug, info, none	debug
transport:debug	Управление режимом отладочного журналирования для RDP-протокола (freerdp-shadow) По умолчанию режим отладочного журналирования выключен. Для включения необходимо присвоить параметру значение true	false
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 RDP-протокола (поставляется с пакетом freerdp)	/usr/libexec/stal/freerdp-shadow-cli
x11rdp:args	Список аргументов для команды RDP-протокола	"/ipc-socket:%{socket}", "/max-connections:1"
tcp:keepalive:enable	Управление механизмом keepalive по протоколу TCP. Механизм keepalive помогает разорвать зависшее соединение с минимальным временем ожидания. При значении false подключение к сессии после разрыва соединения и его восстановления возможно только по прошествии некоторого времени. При значении true подключение к сессии после разрыва соединения возможно сразу после его восстановления	true
tcp:keepalive:delay	Время (в секундах) простоя соединения, по прошествии которого TCP начнёт отправлять проверочные пакеты	5
tcp:keepalive:retries	Максимальное число проверок 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`:

```

1  {
2      "debug:level": "debug",
3
4      "#runtime:dir": "/run/stal",
5      "#runtime:xdg": "/run/user/%{uid}",
6
7      "#xvfb:path": "/usr/bin/Xorg",
8      "#xvfb:args": [ ":%{display}", "-nolisten", "tcp", "-logfile", "/dev/null",
9      "-auth", "%{authfile}", "-config", "stal.conf", "-depth", "%{depth}",
10     "+extension", "DAMAGE", "+extension", "MIT-SHM", "+extension", "RANDR",
11     "+extension", "XFIXES", "+extension", "XTEST" ],
12     "#xvfb:sock": "/tmp/.X11-unix/X%{display}",
13
14     "#pam:service": "stal",
15
16     "users:limit": 200,
17     "sessions:limit": 1000,
18
19     "#groups:allow": [],
20
21     "session:path": "/usr/bin/fly-wm",
22     "session:args": [ ],
23     "session:programs": "/etc/stal/programs.json",
24
25     "#seamless:timeout": 60,
26     "#inactivity:timeout": 0,
27     "#duration:timeout": 0,
28     "#disconnect:timeout": 0,
29     "#clipboard:limit": 0,
30
31     "#redirect:drive": true,
32     "#redirect:print": true,
33     "#redirect:smartcard": true,
34     "#clipboard:file": true,
35     "#clipboard:server": true,
36     "#clipboard:client": true,
37
38     "#connect:policy": "PrevReplace",
39     "#session:disconnected:freeze": false,
40
41     "#rdp:keepalive:interval": 0,
42     "#rdp:keepalive:failures": 0,

```

```

40
41     "applications:skip": [ "lcestart.desktop" ],
42
43     "#helper:notification": "/usr/libexec/stal/stal_notify",
44     "#xrandr:path": "/usr/bin/xrandr",
45
46     "#tdsk:enable": false,
47     "#tdsk:fstype": "ext4",
48     "#tdsk:option": ""
49 }
    
```

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
<code>debug:level</code>	Уровень отладочных сообщений. Возможные значения: <code>debug</code> , <code>info</code> , <code>none</code>	<code>debug</code>
<code>runtime:dir</code>	Рабочий каталог сервиса STAL	<code>/run/stal</code>
<code>runtime:xdg</code>	XDG-каталог сессии	<code>/run/user/{uid}</code>
<code>xvfb:path</code>	Путь запуска X11-сервера	<code>/usr/lib/xorg/Xorg</code>
<code>xvfb:args</code>	Список аргументов X11-сервера. Возможны подстановки служебных значений: <code>{display}</code> , <code>{authfile}</code> , <code>{depth}</code> , <code>{width}</code> , <code>{height}</code>	Не задано
<code>xvfb:sock</code>	Формат сокета для X11-сервера Возможна подстановка служебного значения: <code>{display}</code>	<code>/tmp/.X11-unix/X{display}</code>
<code>pam:service</code>	Идентификатор сервиса доступа PAM	<code>stal</code>
<code>users:limit</code>	Ограничение на количество пользователей, подключившихся к STAL	<code>200</code>
<code>sessions:limit</code>	Ограничение на количество сессий, запущенных на STAL	<code>1000</code>
<code>groups:allow</code>	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: <code>"groups:allow":["group1", "group2"]</code>	<code>[]</code>
<code>session:path</code>	Клиентская программа, запускаемая в сессии	<code>/usr/bin/fly-wm</code>
<code>session:args</code>	Список аргументов для запуска клиентской программы	Не задано
<code>session:programs</code>	Файл списка разрешенных программ для режима <code>seamless</code> , формат <code>json</code>	<code>/etc/stal/programs.json</code>

Параметр	Назначение	Значение по умолчанию
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
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: <ul style="list-style-type: none"> ▪ 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
applications:skip	Список запрещенных программ, которые не будут опубликованы. В значении параметра должен указываться ярлык программы: <имя программы>.desktop	1cestart.desktop

Параметр	Назначение	Значение по умолчанию
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».

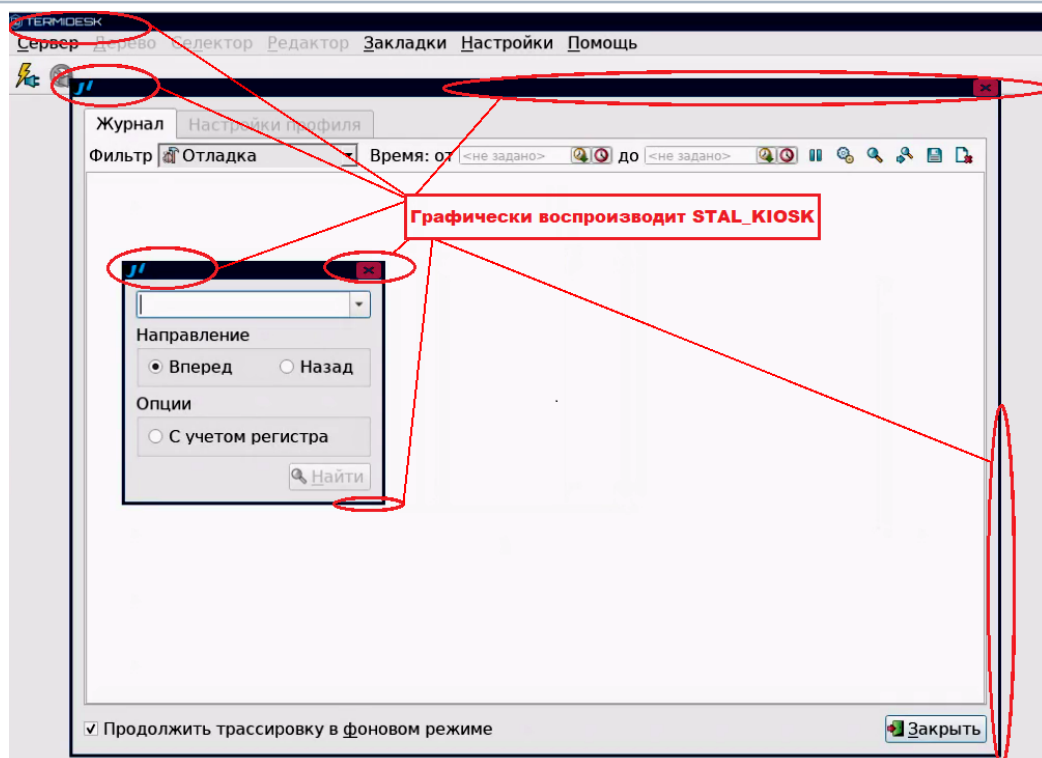


Рисунок 1 – Влияние stal_kiosk на поведение окна

Пример файла /etc/stal/stal_kiosk.json:


```

1  [
2      {
3          "wm:window:type": "dialog",
4          "wm:class": "1cv8*",
5          "wm:window:role": "GtkFileChooserDialog",
6          "frame": false,
7          "fullscreen": true
8      },
9      {
10         "wm:window:type": "dialog",
11         "wm:class": "1cv8*",
12         "frame": false,
13         "fullscreen": false
14     },
15     {
16         "wm:class": "xterm",
17         "frame": false,
18         "fullscreen": true
19     },
20     {
21         "wm:window:type": "normal",
22         "wm:class": "*",
23         "frame": false,
24         "fullscreen": true
25     },
26     {
27         "wm:window:type": "dialog",
28         "wm:class": "*",
29         "frame": true,
30         "fullscreen": false
31     }
32 ]
    
```

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

Для получения значения тега для определенного окна нужно:

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

```

:~$ xrpor
    
```

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

```

1  WM_NAME(COMPOUND_TEXT) = "Домашняя - Менеджер файлов"
2  _NET_WM_NAME(UTF8_STRING) = "Домашняя - Менеджер файлов"
3  _MOTIF_WM_HINTS(_MOTIF_WM_HINTS) = 0x3, 0x3e, 0x7e, 0x0, 0x0
4  _NET_WM_WINDOW_TYPE(ATOM) = _NET_WM_WINDOW_TYPE_NORMAL
    
```

```

5  _XEMBED_INFO(_XEMBED_INFO) = 0x0, 0x1
6  WM_CLIENT_LEADER(WINDOW): window id # 0x3200008
7  WM_HINTS(WM_HINTS):
8      Client accepts input or input focus: True
9      window id # of group leader: 0x3200008
10 WM_CLIENT_MACHINE(String) = "cl-00000"
11 _NET_WM_PID(CARDINAL) = 1721
12 _NET_WM_SYNC_REQUEST_COUNTER(CARDINAL) = 52429217
13 WM_CLASS(String) = "fly-fm-service", "fly-fm-service"
14 WM_PROTOCOLS(ATOM): protocols WM_DELETE_WINDOW, WM_TAKE_FOCUS, _NET_WM_PING,
    _NET_WM_SYNC_REQUEST
15 WM_NORMAL_HINTS(WM_SIZE_HINTS):
16     user specified size: 1333 by 913
17     program specified minimum size: 182 by 219
18     window gravity: Static
    
```

Таблица 4 – Описание параметров файла конфигурации stal_kiosk

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

- 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).

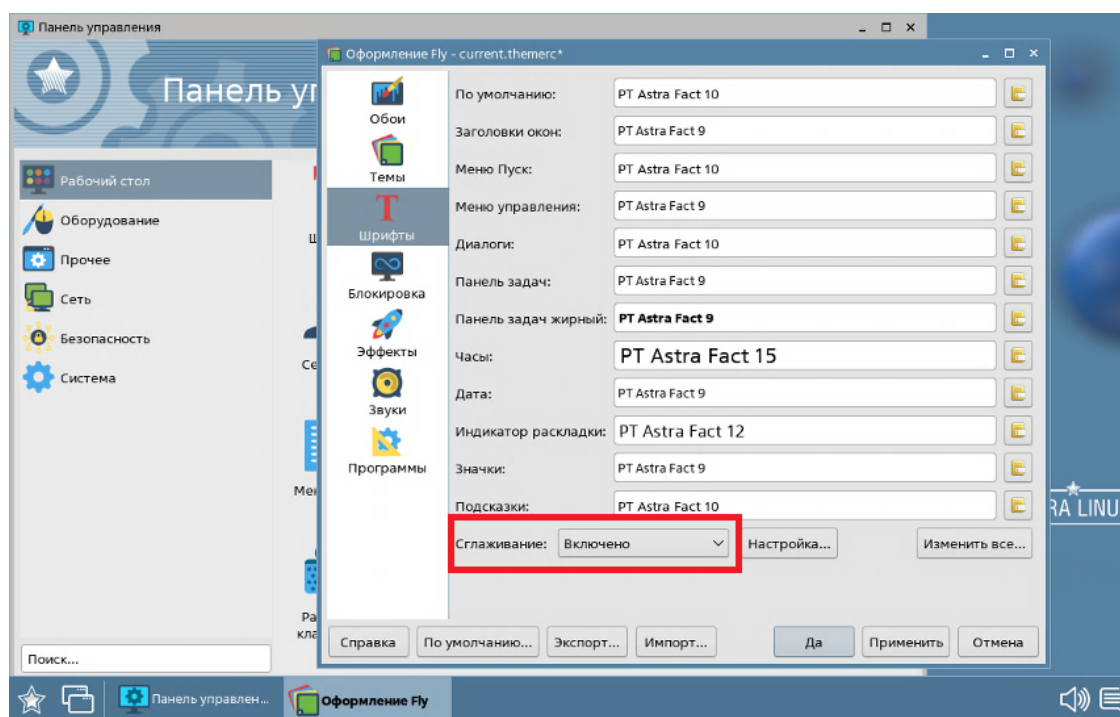


Рисунок 2 – Включение сглаживания шрифтов

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

```

1 Modeline "8192x4096" 252.50 8192 8400 9216 10240 4096 4099 4109 4113 -hsync
+vsync
2 Modeline "5496x1200" 257.25 5496 5696 6256 7016 1200 1203 1213 1224 -hsync
+vsync
3 Modeline "5280x1080" 262.00 5280 5496 6032 6784 1080 1083 1093 1105 -hsync
+vsync
    
```

4	Modeline "5280x1200"	284.75	5280	5512	6056	6832	1200	1203	1213	1226	-hsync	+vsync
5	Modeline "5120x3200"	277.75	5120	5344	5872	6624	3200	3203	3209	3227	-hsync	+vsync
6	Modeline "4800x1200"	267.00	4800	5016	5512	6224	1200	1203	1213	1227	-hsync	+vsync
7	Modeline "3840x2880"	297.50	3840	4072	4472	5104	2880	2883	2887	2916	-hsync	+vsync
8	Modeline "3840x2560"	262.00	3840	4048	4448	5056	2560	2563	2573	2592	-hsync	+vsync
9	Modeline "3840x2048"	262.75	3840	4048	4448	5056	2048	2051	2061	2080	-hsync	+vsync
10	Modeline "3840x1080"	283.25	3840	4064	4464	5088	1080	1083	1093	1114	-hsync	+vsync
11	Modeline "3600x1200"	296.75	3600	3824	4200	4800	1200	1203	1213	1238	-hsync	+vsync
12	Modeline "3440x1440"	270.00	3440	3648	4008	4576	1440	1443	1453	1476	-hsync	+vsync
13	Modeline "3288x1080"	296.00	3288	3504	3848	4408	1080	1083	1093	1120	-hsync	+vsync
14	Modeline "2048x2048"	295.25	2048	2208	2424	2800	2048	2051	2061	2109	-hsync	+vsync
15	Modeline "2048x1536"	267.25	2048	2208	2424	2800	1536	1539	1543	1592	-hsync	+vsync
16	Modeline "2560x1600"	286.00	2560	2744	3016	3472	1600	1603	1609	1649	-hsync	+vsync
17	Modeline "2560x1440"	256.25	2560	2736	3008	3456	1440	1443	1448	1484	-hsync	+vsync
18	Modeline "1920x1440"	233.50	1920	2064	2264	2608	1440	1443	1447	1493	-hsync	+vsync
19	Modeline "1920x1200"	193.25	1920	2056	2256	2592	1200	1203	1209	1245	-hsync	+vsync
20	Modeline "1920x1080"	173.00	1920	2048	2248	2576	1080	1083	1088	1120	-hsync	+vsync
21	Modeline "1680x1050"	146.25	1680	1784	1960	2240	1050	1053	1059	1089	-hsync	+vsync
22	Modeline "1600x1200"	161.00	1600	1712	1880	2160	1200	1203	1207	1245	-hsync	+vsync
23	Modeline "1600x900"	118.25	1600	1696	1856	2112	900	903	908	934	-hsync	+vsync
24	Modeline "1440x900"	106.50	1440	1528	1672	1904	900	903	909	934	-hsync	+vsync
25	Modeline "1368x768"	85.25	1368	1440	1576	1784	768	771	781	798	-hsync	+vsync
26	Modeline "1280x1024"	109.00	1280	1368	1496	1712	1024	1027	1034	1063	-hsync	+vsync
27	Modeline "1360x768"	84.75	1360	1432	1568	1776	768	771	781	798	-hsync	+vsync
28	Modeline "1280x800"	83.50	1280	1352	1480	1680	800	803	809	831	-hsync	+vsync
29	Modeline "1280x768"	79.50	1280	1344	1472	1664	768	771	781	798	-hsync	+vsync
30	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:

```

1  [
2      {
3          "name": "наименование приложения",
4          "path": "путь для запуска приложения" ,
5          "args": [ "аргумент запуска 1", ..., "аргумент запуска N" ],
6      }
7  ]
    
```

Пример файла:

```

1  [
2      {
3          "name": "Midnight Commander",
4          "path": "/usr/bin/xterm",
5          "args": [ "-e", "/usr/bin/mc" ]
6      },
7      {
8          "name": "Chromium Gost",
9          "path": "/usr/bin/chromium-gost",
10         "args": []
11     }
12 ]
    
```

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

⚠ Несистемные программы, которые требуют 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:

```

1  #!/bin/bash
2  export PATH=$PATH:/opt/rubackup/bin
3  export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/rubackup/lib
4
5  /opt/rubackup/bin/rbm
6
7  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:

- 1С:Enterprise x64;
- 1С:Enterprise - Thin client x64;
- 1С: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

В 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`, которая запускается 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: <pre> :~\$ sudo loginctl list-sessions </pre> Для получения статуса сессии можно выполнить команду: <pre> :~\$ sudo loginctl session-status <номер сессии> </pre>
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:

```

1  {
2      "default": {

```

```

3         "cpu:weight": 0,
4         "cpu:quota": 0,
5         "memory:high": "",
6         "memory:max": "",
7         "task:max": 0,
8         "network:deny": "",
9         "network:allow": ""
10    },
11
12    "groups": [
13        {
14            "name": "test-admins",
15            "cpu:weight": 0,
16            "cpu:quota": 0,
17            "memory:high": "",
18            "memory:max": "",
19            "task:max": 1024
20        },
21        {
22            "name": "test-users",
23            "cpu:weight": 0,
24            "cpu:quota": 20,
25            "memory:high": "2G",
26            "memory:max": "3G",
27            "task:max": 256
28        }
29    ],
30
31    "users": [
32        {
33            "name": "vasyan",
34            "cpu:weight": 0,
35            "cpu:quota": 3,
36            "memory:high": "1G",
37            "memory:max": "2G",
38            "task:max": 128,
39            "network:deny": "any",
40            "network:allow": "localhost"
41        }
42    ]
43 }
```

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).

i 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
<code>name</code>	Имя группы или пользователя, к которому будут применены ограничения
<code>cpu:weight</code>	Соответствует параметру « <code>CPUWeight</code> » в системе управления службами <code>systemd</code> . Разрешенные значения от 1 до 10000, по умолчанию <code>systemd</code> задает 100. Значение «0»: функциональность не используется.
<code>cpu:quota</code>	Соответствует параметру « <code>CPUQuota</code> » в системе управления службами <code>systemd</code> . Значение указывается в процентах на одно ядро процессора. Значение «0»: функциональность не используется
<code>memory:high</code>	Ограничение использования памяти выполняемыми процессами. Ограничение может быть превышено, если это неизбежно, но в таких случаях процессы сильно замедляются. Соответствует параметру « <code>MemoryHigh</code> » в системе управления службами <code>systemd</code> . Значение задается в байтах. Также могут быть использованы суффиксы: <ul style="list-style-type: none"> ▪ К - килобайт, например: 1K; ▪ М - мегабайт, например: 1M; ▪ G - гигабайт, например: 1G; ▪ Т - терабайт, например: 1T. Значение не задано: параметр и функциональность не используются
<code>memory:max</code>	Абсолютное ограничение использования памяти выполняемыми процессами. Если ограничение превышает, будет вызвано системное средство устранения нехватки памяти. Соответствует параметру « <code>MemoryMax</code> » в системе управления службами <code>systemd</code> . Значения задаются аналогично параметру <code>memory:high</code> . Значение не задано: функциональность не используется
<code>task:max</code>	Максимальное количество задач, которые можно создать для сессии. Соответствует параметру « <code>TasksMax</code> » в системе управления службами <code>systemd</code> . Значение «0»: функциональность не используется
<code>network:deny</code>	Соответствует параметру « <code>IPAddressDeny</code> » в системе управления службами <code>systemd</code> . В качестве значений можно указывать: <ul style="list-style-type: none"> ▪ разделенный пробелами список IP-адресов, каждый из которых может иметь значение маски после символа «/», например: 192.0.2.1/24; ▪ символическое имя «<code>any</code>»: любой узел; ▪ символическое имя «<code>localhost</code>»: локальный узел; ▪ символическое имя «<code>link-local</code>»: все локальные IP-адреса; ▪ символическое имя «<code>multicast</code>»: все IP-адреса многоадресной рассылки. Значение не задано: функциональность не используется

Параметр	Назначение
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 . Перенаправление ресурсов

3.7.1 . Общие сведения

В текущей версии STAL поддерживает:

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

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


При подключении высокоуровневым пользователем перенаправление ресурсов работать не будет - это блокируется защитными механизмами ОС Astra Linux Special Edition.

Не поддерживается перенаправление ресурсов для ОС Astra Linux Special Edition уровня защищенности «Смоленск».

Правила перенаправления ресурсов для терминальных сессий задаются политиками фонда на сервере Termidesk (см. подраздел **Политики фонда ВРМ** документа СЛЕТ.10001-02 90 02 «Руководство администратора. Настройка программного комплекса»).

3.7.2 . Перенаправление принтеров в сервер терминалов STAL

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

 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 формата RAW без изменения отправится на рабочую станцию 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.

3.7.3 . 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>`.

3.7.4 . 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.

3.8 . Журналирование

STAL интегрирован с инструментом мониторинга событий и журналирования `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:

```
1 :~$ sudo journalctl -t stal_proxy
2 :~$ sudo journalctl -t stal_service
3 :~$ sudo journalctl -t stal_rdpepc
```

```
4 :~$ sudo journalctl -t stal_watchdog
```

3.9 . 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 того, чтобы сформировать файл архива с журналами, необходимо выполнить:

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

В результате выполнения команды создается файл `/var/tmp/stal_report_YYYYMMDD_HHMMI.tgz`, где YYYY - год, MM - месяц, DD - день, HH - часы, MM - 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 нестандартных ситуаций

Индикация	Описание	Возможное решение
Ошибка: «Ошибка сервера»	Ошибка появляется при попытке соединения к STAL	Ошибка появляется при установленном пакете <code>xserver-xorg-legacy</code> и связана со значением параметра <code>allowed_users</code> в файле <code>/etc/X11/Xwrapper.config</code> . Параметру необходимо присвоить значение <code>anybody</code> . 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 <code>termidesk-session-agent</code>	Необходимо проверить журнал событий <code>/var/log/termidesk/stal_service.log</code> на наличие записей «Error from reader» и «Missing in array declaration». Наличие ошибок свидетельствует, что в файле <code>/etc/stal/programs.json</code> 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 вошел 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 $\geq 1.7.5$ 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 <code>xrdp</code> на сервере STAL. Если он установлен, его необходимо удалить, поскольку <code>xrdp</code> занимает порт 3389, на котором работает STAL
Нет подключения при попытке получить опубликованное приложение	При попытке получить опубликованное приложение возникает черный экран, подключения нет. STAL находится в домене Microsoft Active Directory	Необходимо проверить журнал событий <code>/var/log/termidesk/stal_service.log</code> 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

Индикация	Описание	Возможное решение
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»

5. ПРИНЯТЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин	Определение
Виртуальное рабочее место	Также: ВРМ. Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа
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 ВРМ
Протокол доставки	Поддерживаемый в Termidesk протокол удаленного доступа к ВРМ
Компонент «Сессионный агент»	Компонент Termidesk. Устанавливается на сервер терминалов (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 ВРМ и контроля доставки ВРМ. Устанавливается из пакета termidesk-vdi. Наименование службы после установки: termidesk-vdi.service
Фонд рабочих мест	Также: фонд ВРМ. Совокупность подготовленных ВРМ 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 ВРМ с ОС Astra Linux Special Edition через сеанс удаленного терминала

6. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Пояснение
ВРМ	Виртуальное рабочее место
ОС	Операционная система
ПО	Программное обеспечение
PAM	Pluggable Authentication Module (подключаемый модуль аутентификации)
Termidesk	Программный комплекс «Диспетчер подключений виртуальных рабочих мест Termidesk»
STAL	Terminal Server Astra Linux (сервер терминалов ОС Astra Linux Special Edition (Server))



© ООО «УВЕОН»

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