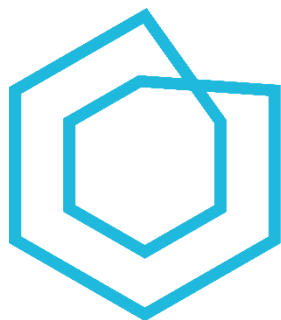


ООО «ВЭБ КОНТРОЛ ДК»



sPACE

**СИСТЕМА УПРАВЛЕНИЯ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ
sPACE RAM**

ВЕРСИЯ 2.0.2

ИНСТРУКЦИЯ ПО РАЗВЕРТЫВАНИЮ 2.0.2

Москва, 2025

СОДЕРЖАНИЕ

1. Введение	3
1.1. Общие положения	3
1.2. Термины и сокращения	3
2. Назначение СУПД sPACE RAM	4
2.1. Архитектура СУПД	4
3. Требования	5
3.1. Требования к аппаратному обеспечению серверной части	5
3.2. Требования к программному обеспечению серверной части	5
3.3. Требования к аппаратному обеспечению рабочих станций	6
3.4. Требования к программному обеспечению рабочих станций	6
3.5. Требования к инфраструктуре	7
3.6. Требования к сетевой доступности	8
4. Состав дистрибутива	9
5. Установка СУПД sPACE RAM	10
5.0 Подготовка к установке	10
5.1 Установка на Linux	11
5.2 Первая авторизация на портале	14
5.3 Добавление пользователей с правами администратора	15
5.4 Загрузка лицензии и смена пароля администратора	17
5.5 Установка сервера ЗСА	19
5.6 Введение сервера ЗСА в используемые	21
5.7 Дополнительная настройка для сервера ЗСА Windows	24
5.7.3. Рекомендации для ЗСА Windows	28
5.8 Настройка групповых политик ЗСА Windows	32
6. Настройка отказоустойчивой системы	37
6.1. Схема отказоустойчивой системы	37
6.2. Процесс установки второго (или N-го) Ядра системы	38
7. Список стороннего ПО	39
Приложение 1: Чек-лист подготовки инфраструктуры	40

1. Введение

1.1. Общие положения

Настоящая инструкция предназначена для лиц, осуществляющих установку и настройку Системы управления привилегированным доступом sPACE, а также программного обеспечения, необходимого для её функционирования.

Инструкция не заменяет учебную, справочную литературу, руководства от производителя операционной системы и стороннего программного обеспечения (ПО).

1.2. Термины и сокращения

Используемые в настоящей инструкции термины и сокращения представлены в Таблице 1:

Таблица 1 «Термины и сокращения»

Сокращение	Термин – Описание
СУПД	Среда Управления Привилегированным Доступом – программно-аппаратный комплекс, предназначенный для управления и контроля над действиями администраторов ОА .
sPACE	Safe Privileged Access Control Environment – английское название СУПД .
ОА	Объект Администрирования – целевая система, где производятся административные действия.
ЗСА (или ЗС)	Защищенная Среда Администрирования (или Сервер Защищенной Среды) – выделенный сервер, на котором выполняется сеанс администрирования.
ИА	Инструмент Администрирования – приложение, запускаемое на сервере ЗСА , с помощью которого осуществляются административные действия в ОА .
СОС	Служба Обмена Сообщениями – служба, обеспечивающая коммуникацию между компонентами СУПД .

При возникновении проблем при развертывании и настройке смотрите также базу знаний **FAQ sPACE** по адресу <https://webcontrol.aspro.cloud/hc/3>

2. Назначение СУПД sPACE PAM

Система Управления Привилегированным Доступом sPACE PAM предназначена для того, чтобы управлять и контролировать действия администраторов ОА. СУПД sPACE работает в защищённой среде и позволяет пользователям подключаться к ней.

2.1. Архитектура СУПД

Пример архитектуры СУПД sPACE, интегрированной с внешними системами, изображен на Рис. 1.

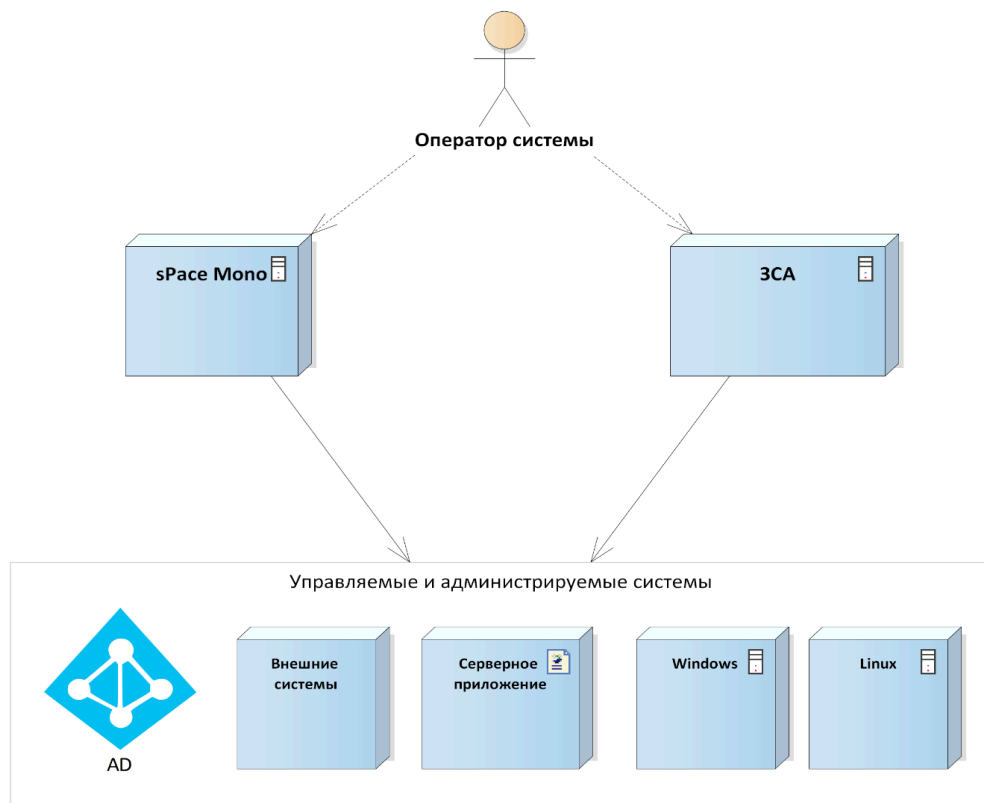


Рис. 1. Архитектура

Состав серверного оборудования:

- *sPACE Mono (Base)* — комплексная инсталляция на одном сервере, реализующая ролевую модель доступа, процессы аутентификации и авторизации пользователей, запуск сеансов администрирования, аудит сеансов администрирования, настройку системы;
- *Сервер ЗСА* — реализует защищённую среду для сеанса администрирования;
- *Active Directory (AD)* — службы каталогов для операционных систем семейства Windows Server. Используется СУПД для аутентификации и авторизации пользователей;
- *Внешние системы*, взаимодействие с которыми поддерживает система СУПД sPACE PAM. Например, *Observe It* или *Beyond Trust Privileged Identity*.
- *Серверное приложение* — прикладное программное обеспечение, использующее различные механизмы аутентификации, которые имеют консоль управления, представленную как клиентское ПО в виде веб-интерфейса, командной строки или приложения для ОС.
- *Windows* — ОС Microsoft Windows Server,
- *Linux* — машина на ОС Linux.

3. Требования

3.1. Требования к аппаратному обеспечению серверной части

Таблица 2 «Требования к аппаратному обеспечению серверов»

Сервер	Характеристики физического сервера
Сервер sPACE Mono (Base)	Процессор: 4 ядра, 2,2 ГГц Оперативная память: 8 ГБ Дисковое пространство: 150 ГБ
Сервер ЗСА	Процессор: 4 ядра, 2,2 ГГц Оперативная память: 8 ГБ Дисковое пространство: 150 ГБ
Хранилище архива сессий	Требуется рассчитать дополнительно.

3.2. Требования к программному обеспечению серверной части

Таблица 3 «Требования к программному обеспечению серверов»

Сервер	Состав ПО
Сервер sPACE Mono (Base)	CentOS 7-8, Ubuntu 22.04 и 24.04, Astra Linux «Орёл», Red OS «Муром» 7.3.2, ALT Linux 10; OpenSSL 1.1.1 и выше; Docker 24.0 и выше; Wget (GNU Wget); tar (tape archive); awk; sed (Stream Editor).
Сервер ЗСА Windows	Microsoft Windows Server 2012-2019; Remote Desktop Server (RDS); Windows PowerShell 5.1 и выше.
Сервер ЗСА Linux	CentOS 7-8, Ubuntu 22.04 и 24.04, Astra Linux «Орёл», Red OS «Муром» 7.3.2, ALT Linux 10; <i>Примечание: для запуска на СЗС Linux приложений с графической оболочкой поддерживается только ALT Linux.</i> OpenSSL 1.1 и выше; Docker 24.0 и выше; Expect;

	Wget (GNU Wget); unzip; SSH (Secure Shell).
--	---

3.3. Требования к аппаратному обеспечению рабочих станций

Таблица 4 «Требования к аппаратному обеспечению рабочих станций»

Компонент	Минимальная конфигурация
Процессор	Intel Pentium 1.8 ГГц (или совместимый аналог), число ядер – 2
Оперативная память (RAM)	3 ГБ
Жесткий диск (доступное место на диске)	HDD или SSD, 2 ГБ
Видеоадаптер	Любой
Сетевая плата	Ethernet 100 Мбит/с (рекомендуется 1 Гбит/с)
Дополнительное оборудование	Монитор 1024x768 и больше (рекомендуется 1920x1080), мышь, клавиатура

3.4. Требования к программному обеспечению рабочих станций

Таблица 5 «Требования к программному обеспечению рабочих станций»

Компонент	Конфигурация
Операционная система	Microsoft Windows 7-10, Linux(CentOS 7-8, Ubuntu 18.04, Ubuntu 20.04, Astra Linux «Орёл»), Mac OS 10.11 и выше, iOS 8.0 и выше, Android 4.1 и выше, ...
Прикладное ПО	Microsoft Edge 79.0 и выше; Google Chrome 119.0 и выше; Chromium 121 и выше; Mozilla Firefox 115.0 и выше; Совместимый клиент RDP; Open Secure Shell (для работы с сервером 3CA Linux); Windows PowerShell 5.1 и выше (для работы с сервером 3CA Linux).

3.5. Требования к инфраструктуре

- Если поиск объектов в Active Directory без аутентификации запрещен, то необходима служебная учетная запись, с правами которой СУПД будет осуществлять поиск сотрудников для аутентификации;
- Группы в Active Directory, членство пользователей в которых будет соответствовать ролям в СУПД. Список групп и соответствие роли в СУПД представлен в Таблице 6;
- Перед установкой дистрибутива сервера ядра убедиться, что ядро находится в одном DNS-пространстве (либо имеет видимость DNS-зоны, в которой находятся контроллеры доменов) с тем доменом, к которому мы будем впоследствии подключаться;
- SSL Сертификат (необязательное требование);
- RDP signing сертификат (необязательное требование);

Таблица 6 «Роли в СУПД и их соответствие группам в AD»

Роль	Название в AD	Доступ
Базовый пользователь	SPACE_RESTRICTEDUSERS	Запуск сеансов администрирования.
Стандартный пользователь	SPACE_STANDARDUSERS	Запуск сеансов администрирования. Запрашивание наряда-допуска для себя.
Продвинутый пользователь	SPACE_USERS	Запуск сеансов администрирования. Запрашивание наряда-допуска как для себя, так и для других. Согласование доверенных нарядов-допусков.
Администратор	SPACE_ADMINS	Настройка своего тенанта системы, добавление объектов. Согласование доверенных нарядов-допусков.
Технический администратор	Нельзя назначить доменному пользователю, только внутреннему пользователю SPACE	Настройка тенантов и сущностей системы, которые общие для всех тенантов.
Аудитор	SPACE_AUDITORS	Аудит действий пользователей.

Продвинутый аудитор	SPACE_TRUSTED_AUDITORS	Аудит действий пользователей, включая данные key-log и clipboard.
Привилегированный администратор	SPACE_SUPERADMINS	Перевод системы в аварийный режим.

3.6. Требования к сетевой доступности

Для обеспечения бесперебойного взаимодействия между компонентами, на серверах sPACE Mono и ЗСА должны быть открыты все порты, перечисленные в Таблице 7.

Таблица 7 «Список требуемых к открытию сетевых портов»

Сетевой порт	Получатель	Источник	Комментарии
443	Сервер sPACE Mono (Base)	Рабочее место пользователя	Доступ к веб интерфейсу sPACE
3389	Сервер ЗСА	Рабочее место пользователя	RDP доступ на Jump Server для запуска приложений
22	Сервер ЗСА Linux	Рабочее место пользователя	SSH доступ на Jump Server сервер для организации сессии пользователя
53	DNS Сервер	Сервер sPACE Mono (Base)	Используется для работы с DNS пространством.
135, 139, 445, 389	Active Directory	Сервер ЗСА	Требуемые сетевые порты для включения сервера в домен для аутентификации пользователей
389, 636	Active Directory	Сервер sPACE Mono (Base)	Интеграция с Active Directory, LDAP/LDAPS
Управляемый порт приложения	Целевые ресурсы	Сервер sPACE Mono (Base)	Запуск сценариев смены учетных данных на целевом ресурсе
Управляемый порт приложения	Целевые ресурсы	Сервер ЗСА, Сервер ЗСА Линукс	Подключение целевого инструментария администрирования к выполнению задач на целевом сервере
4222, 443	Сервер sPACE Mono (Base)	Сервер ЗСА	Защищенный транспорт передачи учетных данных, записей сессий и настроек
4222, 4244	Сервер sPACE Mono 1 (Base)	Сервер sPACE Mono 2 (Base)	Требуется для создания отказоустойчивого кластера из двух и более ядер системы
4222, 4244	Сервер sPACE Mono 2 (Base)	Сервер sPACE Mono 1 (Base)	Требуется для создания отказоустойчивого кластера из двух и более ядер системы
5432	Сервер Базы Данных	Сервер sPACE Mono (Base)	Требуется в случае расположения БД вне серверов Ядра

4. Состав дистрибутива

Программный продукт sPACE PAM распространяется в виде архива, доступного для загрузки по индивидуальной ссылке.

В состав дистрибутива системы входят следующие файлы:

- spaceinstall – исполняемый файл, предназначенный для установки на машину Linux, который осуществляет установку компонентов системы sPACE Mono (Base).
- linux_js_installer.gz – архив, с помощью которого осуществляется установка JS Linux.
- space-installer-2.0.2.exe – исполняемый файл, который осуществляет установку JS Windows.

Для работы sPACE необходимо осуществить как минимум одну установку Ядра и одну установку сервера защищенной среды (JS).

5. Установка СУПД sPACE PAM

5.0 Подготовка к установке

Перед началом установки sPACE PAM удостоверьтесь, что выполнены все требования из чек-листа подготовки «Приложение 1». Также поверьте машины, на которые планируется произвести установку. Они должны удовлетворять следующим условиям:

- Установка компонентов sPACE необходимо осуществлять в соответствии с точной последовательностью, изложенной в данной инструкции по развертыванию. То есть, сначала должна осуществляться установка компонента sPACE Mono (пункт «5.1 Установка на Linux»), и лишь затем — установка серверов ЗСА (пункт «5.5 Установка сервера ЗСА»). Также нельзя пренебрегать промежуточными пунктами установки (5.2-5.4), особенно если вы устанавливаете данную систему впервые. При отклонении от последовательности установки, указанной в данной инструкции по развертыванию, корректность установки не гарантируется.
- Все необходимые для работы группы созданы в AD Users and Computers, в них добавлены нужные пользователи. Стандартные названия групп приведены в таблице 6, но при желании их потом можно изменить через интерфейс портала в разделе «Управление ресурсами» > «Пользовательские роли».

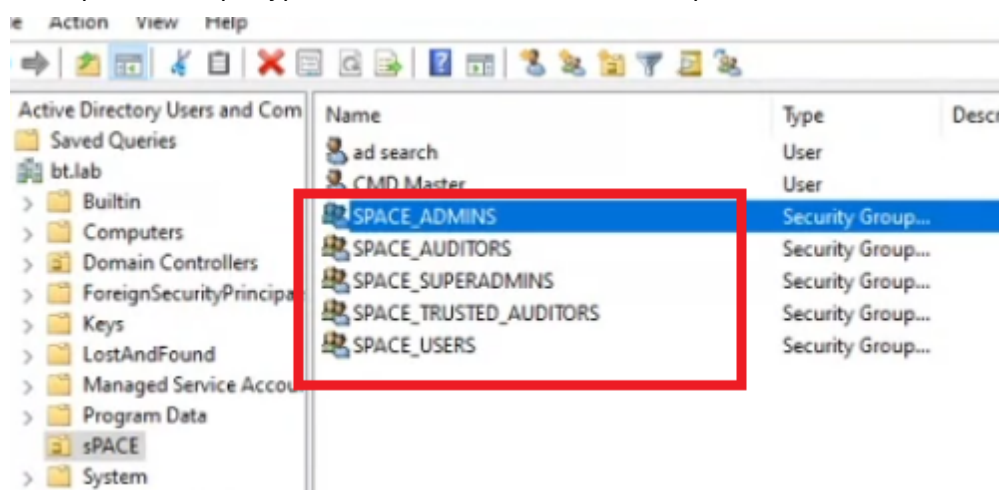


Рис. 2. Пример созданных групп в AD Users and Computers

- На сервере Windows под развертывание ЗСА Windows установлен Remote Desktop Services с установленными Collection.
- Сервер Windows под развертывание ЗСА Windows подключен к тому домену, в котором планируется работа с пользователями, участвующими в тестировании. У этих пользователей есть разрешение на подключение по RDP к данному серверу.
- На сервере Windows под развертывание ЗСА Windows установлена версия PowerShell не ниже 5.1.14409.1029.
- На сервере Linux под развертывание ЗСА Linux установлен инструмент автоматизации Exprect и пакет Openssl не ниже версии 1.1.
- На сервере Linux под развертывание sPACE Mono и на сервере ЗСА Linux установлен и запущен Docker.
- ОС на всех рабочих машинах используют актуальные часовые зоны и подключены к одному NTP-провайдеру, то есть максимально синхронизированы. Это нужно для того, чтобы не было значительного расхождения (до минуты) в системном времени компонентов системы.

- Если при запуске сеанса будет использоваться RDP подключение на сервер ЗСА Linux (работа приложения с графической оболочкой), то на нём должны быть заранее установлены пакеты `xorg-server-common`, `xrdp` и `dwm`. Также такой ЗСА может быть только на ALT Linux

5.1 Установка на Linux

1. Для корректной работы sPACE Mono на сервер должен быть установлен и запущен **Docker** (Пример команды для установки - `dnf install docker-ce docker-ce-cli`, пример команды для запуска - `systemctl enable docker --now`).

2. Также требуется предварительно установить пакет **OpenSSL** не ниже версии 1.1 (Пример команды для установки - `yum -y install openssl openssl-devel`).

3. Перед началом установки нужно авторизоваться (например, при помощи утилиты Putty) на машине Linux, куда будет произведена установка Ядра. Пользователь должен обладать root-правами.

4. Перейти в папку `etc`, а в ней — файл `hosts`. Добавить в файл запись "`127.0.1.1 fqdn`", где `fqdn` — полный адрес этого сервера в системе доменных имен. Запись должна иметь следующий вид:

```
127.0.0.1          localhost    localhost.localdomain  localhost4
localhost4.localdomain4
127.0.1.1 hostname.domainname hostname
```

5. Перейти в корневую папку `root` или `/var/opt` с помощью Midnight commander (команда `mc`) или с помощью командной строки (команда `cd`). Создать папку для установочного файла. Перейти в неё.

6. Нужно перенести в только что созданную папку файл дистрибутива "**spaceinstall**" (например, при помощи команды `wget`, если есть ссылка на этот файл).

7. Запустить выполнение файла при помощи команды `bash полное_имя_файла` (Пример: `bash spaceinstall-2.0.2.5744`)

8. Появится окно, в котором нужно выбрать режим установки «Установка Mono», поставив звездочку при помощи клавиши пробела, затем нажать клавишу `Enter`. Затем откроются несколько информационных окон, где нужно нажимать «Далее» при помощи клавиши `Enter`. В одном из окон надо будет внимательно проверить настройки таймзоны, после чего нажать «Далее» здесь и во всех последующих окнах.

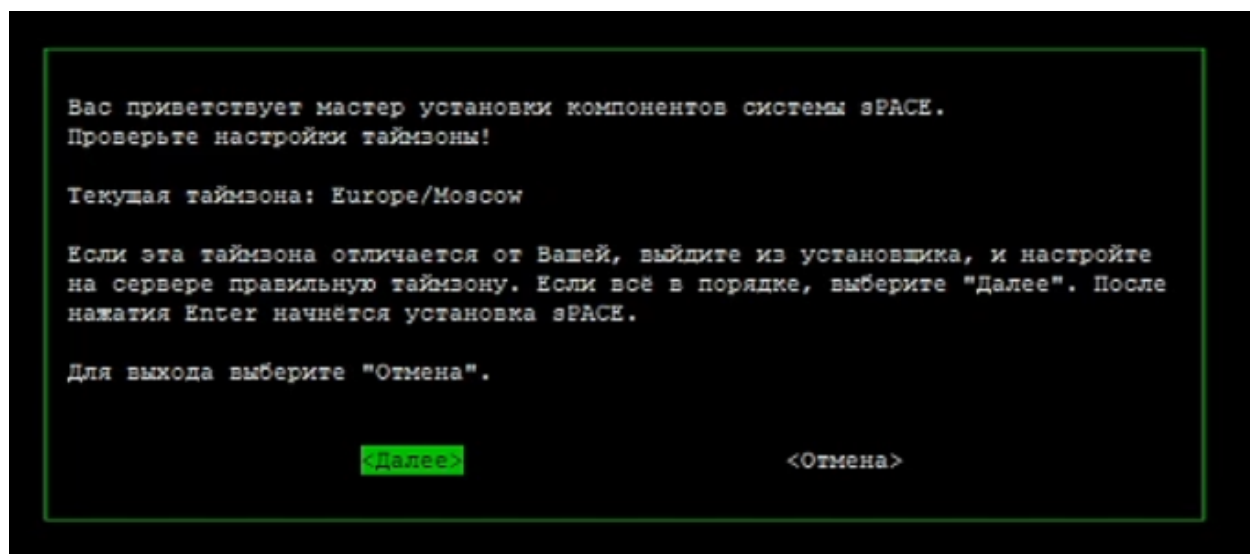
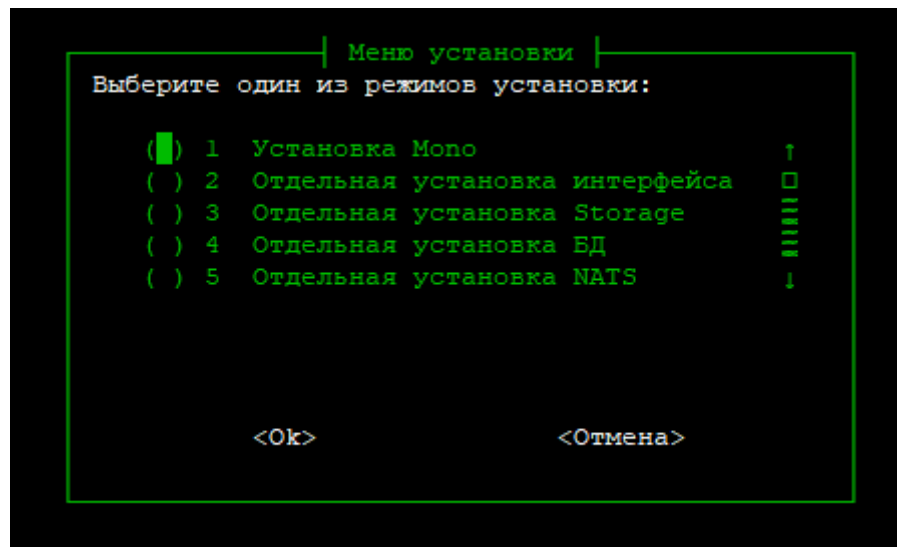
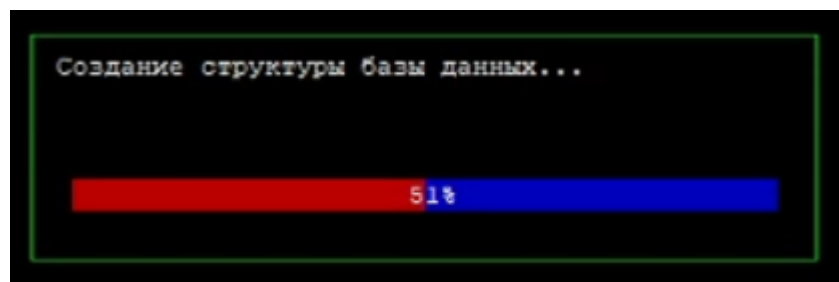
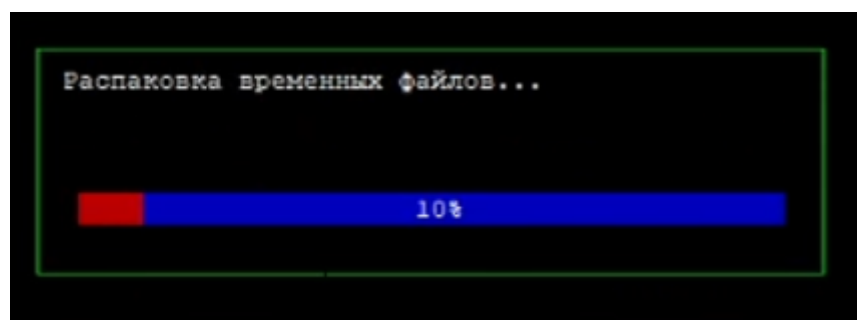


Рис. 3. Начало установки

9. Начнётся процесс установки.



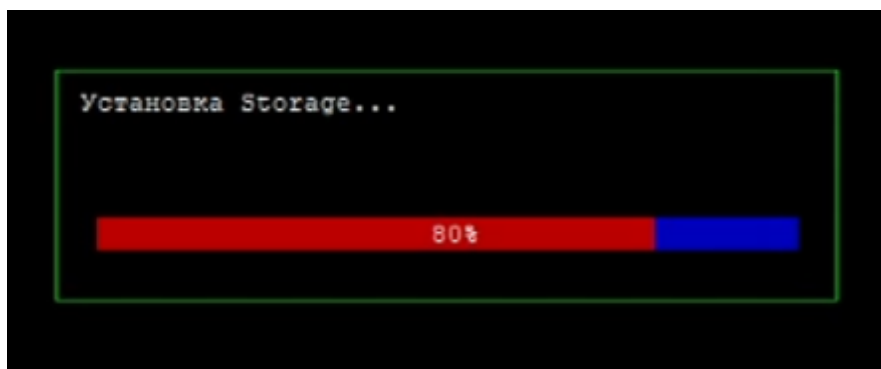


Рис. 4. Процесс установки

10. Как только установка будет завершена, автоматически появится окно с соответствующим уведомлением. Нажать «Ок» чтобы закрыть его и приступить к следующему шагу установки.

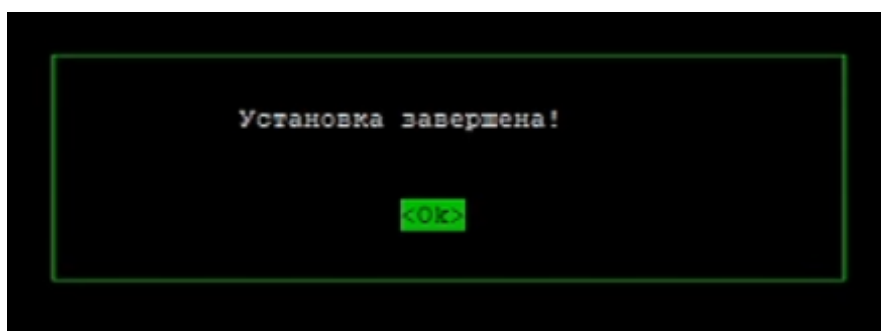


Рис. 5. Завершение установки

11. Убедитесь, что контейнеры из списка ниже запустились, выполнив команду `docker ps`:

Таблица 8 «Список установленных контейнеров»

Образ	Состояние	Имя
tomcat:8.5-jdk8	запущен	spacetomcat8
space/storagebuntu:1	запущен	spacestorage
nats	запущен	nats-server
postgres:9.6	запущен	spacepostgres9

```
[root@testmonoredos spaceinstall]# docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS          NAMES
862a43aa1863   tomcat:8.5-jdk8  "catalina.sh run"       3 minutes ago  Up 3 minutes  spacetomcat8
04c73e32643e   space/storagebuntu:1  "/var/opt/space/ec/s..."  3 minutes ago  Up 31 seconds  spacestorage
a822c2959c29   nats           "/nats-server --conf..."  4 minutes ago  Up 3 minutes  nats-server
6f08964ef2b5   postgres:9.6    "docker-entrypoint.s..."  11 minutes ago  Up 11 minutes  spacepostgres9
```

```
STATUS        PORTS          NAMES
Up 3 minutes  spacetomcat8
Up 31 seconds  spacestorage
Up 3 minutes  nats-server
Up 11 minutes  spacepostgres9
```

Рис. 6. Состояние контейнеров

12. Через одну минуту после завершения установки рекомендуется проверить работоспособность портала. Главная страница портала sPACE PAM с окном входа уже должна быть доступна.

Доступ к веб интерфейсу осуществляется через любой браузер, только по **https** протоколу, то есть <https://IP или DNS имя ядра>.

13. В дальнейшем, при обновлении sPACE PAM до более новых версий, инструкции выполняются в том же порядке. В созданную для дистрибутива папку копируется новый файл “**spaceinstall**” и запускается указанными ранее командами. Произойдет автоматическое резервное копирование. Подтвердить. Откроется окно обновления, в котором следует нажать «Далее».

Как только обновление будет завершено, автоматически появится окно с соответствующим уведомлением.

5.2 Первая авторизация на портале

Авторизуйтесь на портале с использованием стандартного пользователя admin и пароля «admin». Нажмите кнопку «**Вход**».



The login form consists of two input fields: the first is labeled 'Тенант:пользователь@домен' and the second is labeled 'Пароль'. Below these fields are two options: 'Считать пароль с ТМ' and a language dropdown menu set to 'Русский'. At the bottom of the form is a purple button labeled 'Вход'.

Рис. 7. Авторизация на портале

По умолчанию данный пользователь обладает следующими ролями: ROLE_API_MANAGEMENT, ROLE_SPACE_ADMIN, ROLE_SPACE_TECH_ADMIN.

Примечание: Настоятельно рекомендуем не менять роли для пользователя admin, так как он является единственным полноценным администратором на момент первичной установки Системы. Если пользователь потеряет одну из своих ролей, то Систему станет невозможно редактировать. В этом случае поможет только полное удаление и новая установка.

5.3 Добавление пользователей с правами администратора

1. Для создания пользователя-администратора API перейдите в раздел «Управление ресурсами» > «Пользователи».

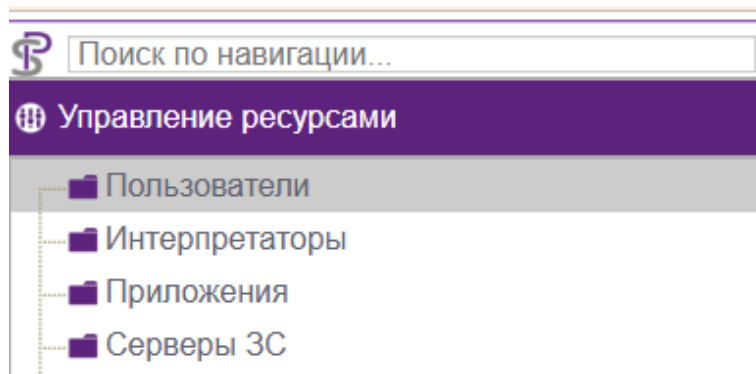


Рис. 8. Местонахождение раздела «Пользователи» в системе

2. Оказавшись в разделе «Пользователи», нажмите на кнопку «Добавить» в верхней панели.

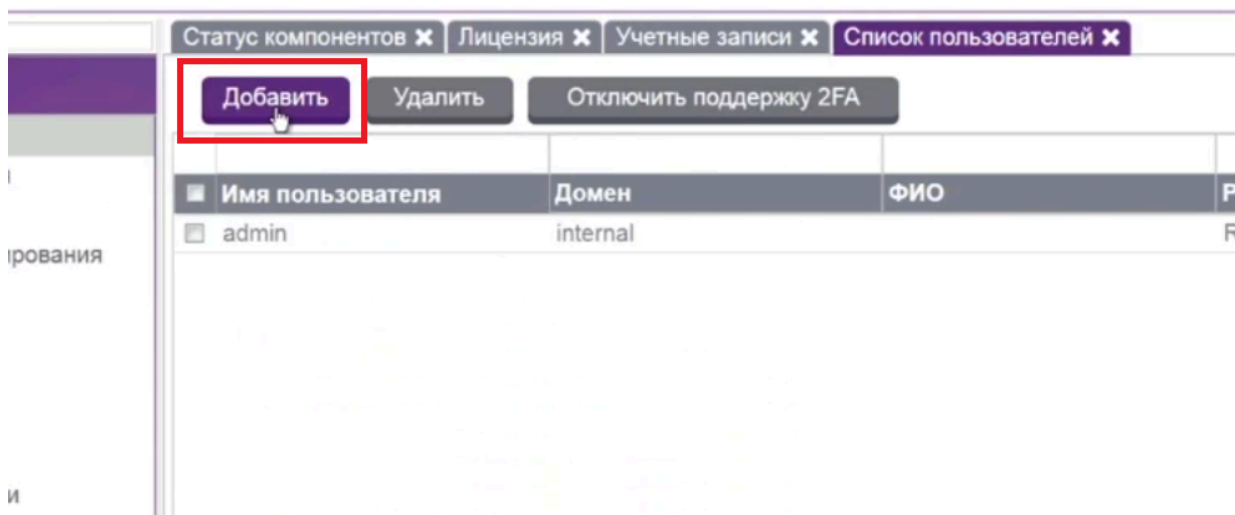


Рис. 9. Кнопка для добавления нового пользователя

3. Откроется окно с формой добавления нового пользователя. Обязательно заполните поля, выделенные полужирным шрифтом: **Имя пользователя** (для корректной работы укажите здесь «sрасе-арі»), **Тенант** (выберите «main»), **Пароль** и **Роли**. Задайте пользователю роль, которая необходима для работы с API: ROLE_API_MANAGEMENT. По желанию вы можете также заполнить поля, которые не являются обязательными. Не нажимайте на кнопку «Ограничить», она предназначена для временной блокировки пользователя и не позволит ему производить какие-либо действия, пока ограничение не будет снято. Закончив, обязательно нажмите на кнопку «Сохранить». Также информацию о добавлении пользователей вы можете прочитать в инструкции на портале, которая открывается при нажатии на серую иконку “i” рядом с полем.

Пользователь

Имя пользователя:

Тенант:

Фамилия:

Имя:

Отчество:

Пароль:

Подтверждение пароля:

Требования: Длина пароля: 6; содержит строчные и прописные буквы; содержит цифры

Ограничить

Мобильный телефон:

Телефон:

Электронный адрес:

Роли:

Сохранить | Сгенерировать пароль | Показать\скрыть пароль | Закрыть

Рис. 10. Форма для добавления нового пользователя

4. После добавления второго администратора API вы можете переходить к созданию пользователей других ролей с правами администратора.

5. Для создания второго технического администратора перейдите в раздел «Управление ресурсами» > «Пользователи».

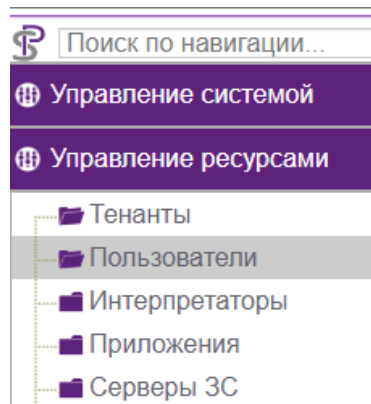


Рис. 11. Местонахождение раздела «Пользователи» в ресурсах

Примечание: Второй пользователь с ролью технического администратора нужен на случай, если пароль от пользователя admin, создаваемого Системой автоматически при инсталляции, будет утерян, либо права этого изначального администратора будут случайно изменены.

6. Далее действуйте по уже описанной схеме: нажмите кнопку «Добавить» в верхней панели, заполните в открывшейся форме имя пользователя и пароль. В списке **Тенант** выберите main. Задайте пользователю роли, необходимые для администрирования системы: ROLE_SPACE_ADMIN и ROLE_SPACE_Tech_ADMIN. Закончив, обязательно нажмите на кнопку «Сохранить».

Рис. 12. Форма добавления нового пользователя

7. После добавления пользователей с правами администраторов вы можете переходить к следующему шагу.

5.4 Загрузка лицензии и смена пароля администратора

1. Перейдите во вкладку «**Лицензия**» в разделе «**Управление ресурсами**». Если лицензия не была предоставлена заранее - нажмите «**Запрос на лицензию**». Будет автоматически сгенерирован и скачан текстовый файл с уникальным license.UUID. Этот файл необходимо направить поставщику Системы для генерации индивидуальной лицензии. Если лицензия уже была предоставлена, переходите к следующему пункту.

2. Во вкладке «**Лицензия**» нажмите «**Загрузка лицензии**», откроется окно загрузки, в котором нужно выбрать файл предоставленной лицензии и нажать «**Загрузить лицензию**».

Рис. 13. Загрузка лицензии

3. Не забудьте поменять пароль для пользователя admin. Это можно сделать в разделе «**Настройки**», который находится в правом верхнем углу рядом с именем пользователя. Нажмите на стрелку, чтобы появилось нужное меню.

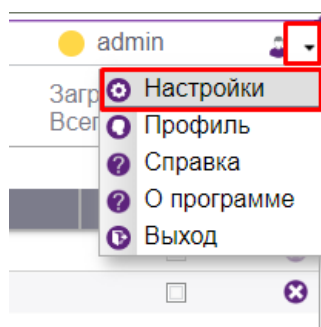
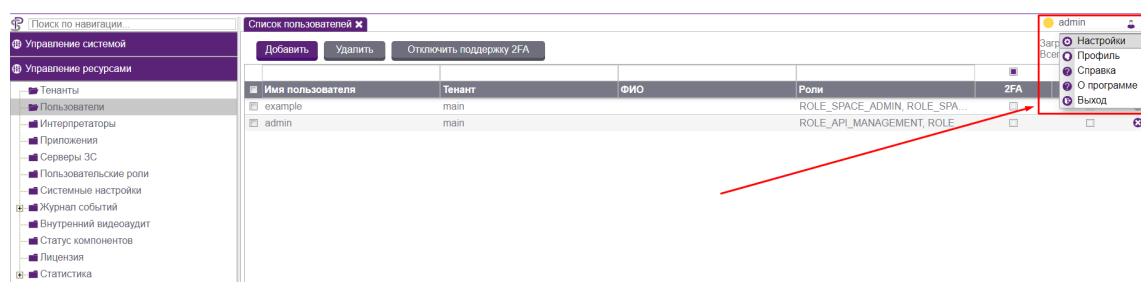


Рис. 14. Местонахождение раздела «Настройки»

4. Откроется окно настроек системы. Перейдите во вкладку «**Безопасность**» и нажмите кнопку «**Сменить пароль**». Поменяйте пароль на более надёжный. Рекомендуется использовать буквы верхнего и нижнего регистра, а также цифры и символы.

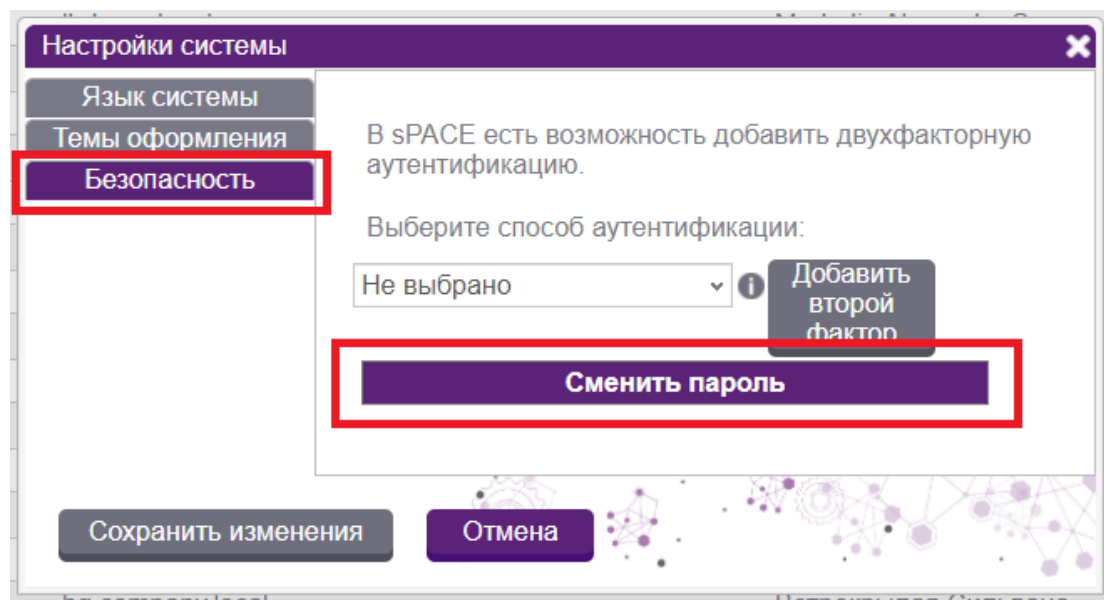


Рис. 15. Окно «Настройки системы»

5. Когда пароль успешно изменен, рекомендуется проверить работоспособность портала. Для этого в меню слева перейдите во вкладке «**Управление ресурсами**» на страницу «**Статус компонентов**». Поле «**Серверы 3С**» должно гореть красным, поскольку серверы 3С еще не были установлены.

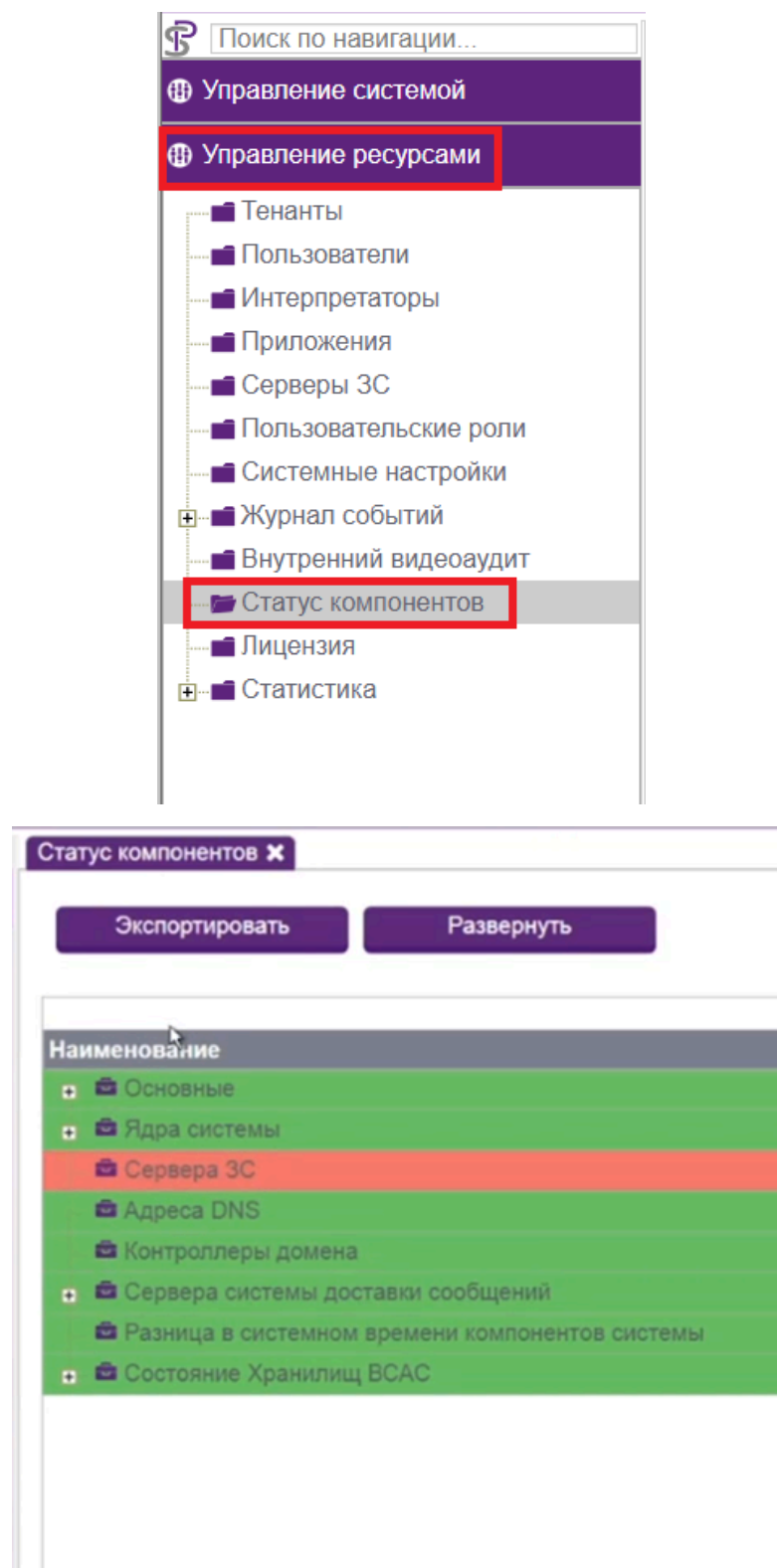


Рис. 16. Вкладка «Статус компонентов»

5.5 Установка сервера 3СА

Сервер 3СА может быть представлен на машине Windows или Linux.

5.5.1 Сервер 3СА Windows

1. Для корректной работы JS Windows на сервере должна быть предварительно установлена роль RDS, включая RD Session Host, RD Connection Broker

(настроены Collection) или терминальный сервер Citrix, для публикации целевого инструментария администрирования целевых пользователей системы.

2. Для начала необходимо авторизоваться с правами администратора на машине Windows, которая будет использоваться как сервер ЗСА Windows. Перенести на неё исполняемый файл **space-installer-2.0.2.exe**. Запустить файл **от имени администратора**. Запустится процесс установки, в появившемся окне нужно ввести IP-адрес инсталляции ядра, указать созданный ранее аккаунт space-api и пароль от него. После ввода нажать клавишу Enter.

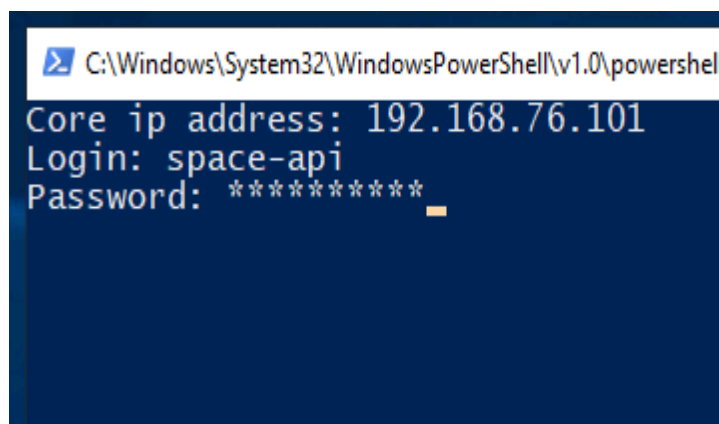
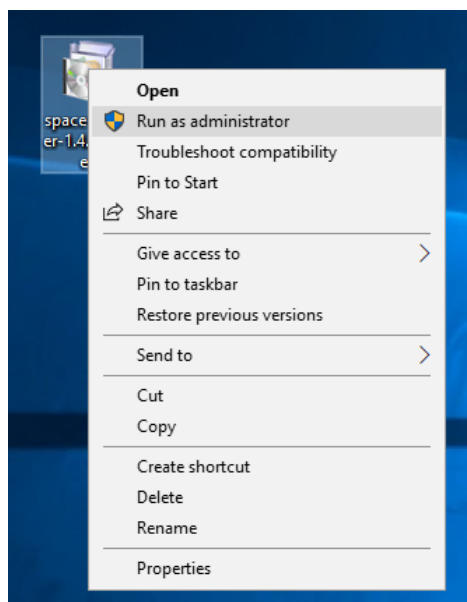


Рис. 17. Запуск от имени администратора

3. Запустится процесс установки. Дождитесь окончания установки.

4. Как только установка завершится, будет показано соответствующее окно. Чтобы выйти из окна установки, нужно нажать клавишу Enter.

5. Установка ЗСА Windows завершена! Далее перейти к установке ЗСА Linux (при необходимости) или пункту введения сервера ЗСА в используемые в веб-интерфейсе.

6. В дальнейшем, при обновлении сервера ЗСА Windows до более новых версий, инструкции выполняются в том же порядке. Перенести на сервер новый исполняемый файл **space-installer-2.0.2.exe** и запустить **от имени администратора**.

5.5.2 Сервер ЗСА Linux

1. Для корректной работы JS Linux на сервер должен быть установлен и запущен **Docker** (Пример команды для установки - `dnf install docker-ce docker-ce-cli`, пример команды для запуска - `systemctl enable docker --now`).

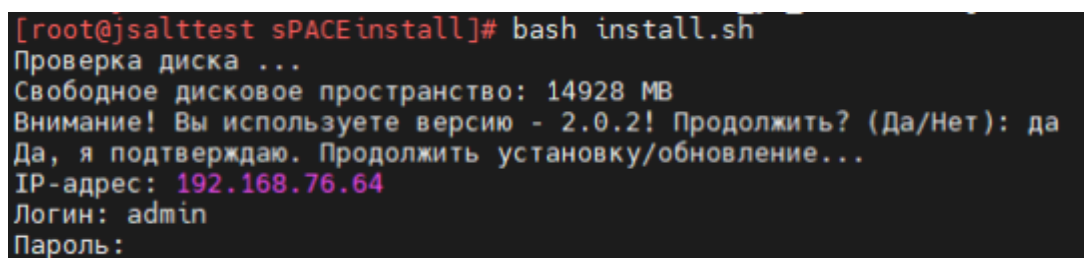
2. Также требуется предварительно установить инструмент автоматизации **Expect** (Пример команды для установки - `dnf install expect`), и пакет **OpenSSL** не ниже версии 1.1 (Пример команды для установки - `yum -y install openssl openssl-devel`) и пакеты **xorg-server-common**, **xrdp** и **dwm**, если при запуске сеанса будет использоваться RDP подключение на сервер ЗСА Linux (работа приложения с графической оболочкой).

3. Для начала установки необходимо авторизоваться под пользователем с правами root на машине Linux, которая будет использоваться как сервер ЗСА, создать по приведенному ранее образцу установочную папку **installer** и перенести в нее архив **linux_js_installer.gz** с компонентами для JS Linux. Разархивировать содержимое каталога **linux_js_installer.gz** (Пример команды для разархивации - `tar -xzf linux_js_installer.gz`).

4. Запустить исполнение файла:

- Обычный режим: `bash install.sh`

После запуска команды необходимо будет подтвердить установку, затем ввести IP-адрес машины с инсталляцией ядра, указать созданный ранее аккаунт space-api и пароль от него.



```
[root@jsaltttest sPACEinstall]# bash install.sh
Проверка диска ...
Свободное дисковое пространство: 14928 МВ
Внимание! Вы используете версию - 2.0.2! Продолжить? (Да/Нет): да
Да, я подтверждаю. Продолжить установку/обновление...
IP-адрес: 192.168.76.64
Логин: admin
Пароль:
```

Рис. 18. Установка в обычном режиме

- Тихий режим: `bash install.sh IP-адрес_машины_с_инсталляцией_ядра space-api пароль_space-api пароль_root_машины_установки`

Пример: `bash install.sh 192.168.74.193 space-api space-api Zaq12wsx`

Дождаться окончания установки. Установка ЗСА Linux завершена! Далее перейти к пункту введения сервера ЗСА в балансировку.

5. В дальнейшем, при обновлении сервера ЗСА Linux до более новых версий инструкции выполняются в том же порядке. В папку **installer** копируется архив **linux_js_installer.gz** с компонентами для JS Linux, проводится разархивация, приведенными ранее командами запускается файл **install.sh**. Система производит обновление.

5.6 Введение сервера ЗСА в используемые

1. При установке дистрибутива на Сервер ЗСА - соответствующий сервер автоматически создается в Системе в разделе «**Неиспользуемые Серверы ЗС**». Чтобы ввести сервер в балансировку авторизуйтесь на портале под пользователем admin. Перейдите во вкладку «**Управление ресурсами**» > «**Серверы ЗС**». Нажмите чекбокс

нужного сервера, убедитесь что отмечен чекбокс «Доступен». Далее нажмите на стрелочку вверх – перенести в используемые.

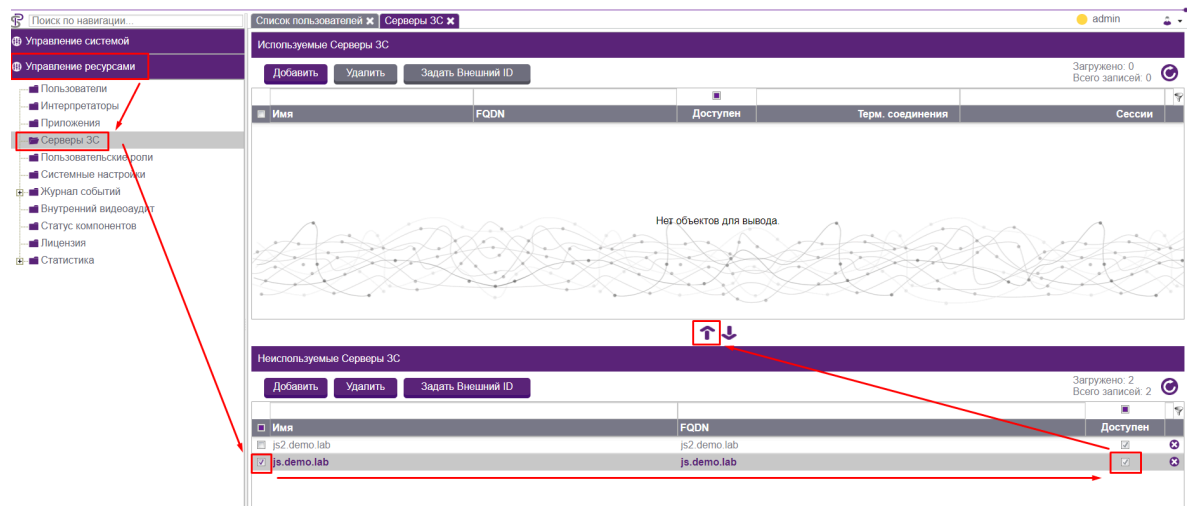


Рис. 19. Введение сервера ЗС в используемые

2. Подтвердить ввод сервера ЗСА в используемые.

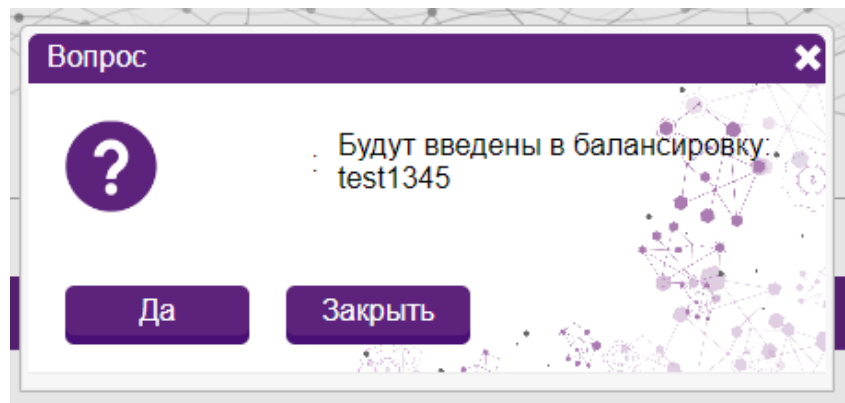


Рис. 20. Пример добавления сервера ЗС в балансировку

3. Обновить табличку серверов ЗС. Убедиться, что у только что созданного сервера ЗС стоит галочка в графе «Доступен».

4. Также стоит проверить тип подключения сервера ЗС. Для этого нужно нажать на него в таблице серверов, открыть карточку и удостовериться, что прописан верный тип подключения.

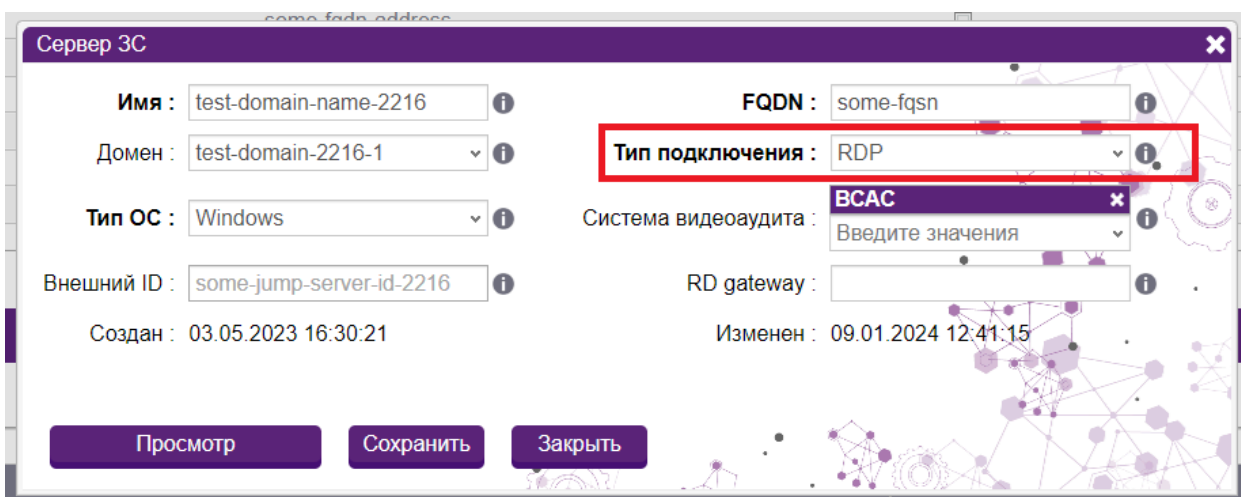


Рис. 21. Пример добавления сервера 3С Windows

Примечание: тип подключения выбирается на основе того, каким будут запускаемые на данном СЗС сеансы.

- Если это будут сеансы с графической оболочкой, то нужно выбирать тип подключения RDP независимо от того, является ли сервер 3С машиной Windows или Linux.
- Если это будут сеансы без графической оболочки, которые запускаются в командной строке рабочей машины пользователя, то нужно выбирать тип подключения SSH.

Ниже представлена более подробная сводная таблица с информацией о разных ОС, типах подключения и типах файлов, которые будут использованы для запуска сеанса.

Таблица 9 «Выбор типа подключения»

Тип сервера 3С	Тип подключения	Тип рабочей машины пользователя	Файл подключения
Windows	RDP	Windows	RDP файл для СЗС Windows
Linux	RDP	Windows	RDP файл для СЗС Linux
Windows	RDP	Linux	Строка XfreeRdp для СЗС Windows
Linux	RDP	Linux	Строка XfreeRdp для СЗС Linux
Windows	SSH	Windows, Linux	-

Тип сервера ЗС	Тип подключения	Тип рабочей машины пользователя	Файл подключения
Linux	SSH	Windows	ps1 файл
Linux	SSH	Linux	Строка SSH
Windows	Citrix	Windows, Linux	ica файл
Linux	Citrix	Windows, Linux	-

Примечание: если нужен сервер ЗС Linux, который будет одновременно поддерживать графические и текстовые сеансы, необходимо вручную добавить еще один тип подключения через интерфейс портала. Для этого используйте форму редактирования сервера ЗС (см. картинку ниже).

Рис. 22. Сервер ЗС, поддерживающий два типа подключения

Далее требуется только настроить Объекты администрирования. Приложения с графической оболочкой должны запускаться на сервере ЗС с подключением RDP, а приложения без графической оболочки — на сервере ЗС с подключением SSH.

5.7 Дополнительная настройка для сервера ЗСА Windows

5.7.1 Настройка приложений

Для того чтобы в Системе работал запуск приложений, используемых в сценариях, соответствующие приложения должны быть установлены на сервере ЗС. Под установку рабочего ПО мы рекомендуем создать на диске С отдельную папку с именем “application”. Путь расположения файла запуска для каждого приложения требуется указывать отдельно в большинстве сценариев для запуска. Например, в сценарии Putty используется путь запуска C:\application\putty\putty.exe -

соответственно, на сервере 3С Putty должен располагаться по этому пути, либо необходимо изменить расположение файла в сценарии.

5.7.2 Настройка приложения “launcher.exe”

Проверьте, есть ли у вас опубликованное приложение “**launcher.exe**”. Если его нет, то перейдите в мастер публикации нового RemoteApp и выполните следующие шаги:

1. Перейдите во вкладку “**Remote Desktop Services**”.
2. Выберите вкладку “**Collections**” и щелкните по вашей коллекции.
3. Нажмите на кнопку “**TASK**” в разделе “**Properties**” и в выпадающем меню нажмите “**Edit Properties**”.
4. В открывшемся окне настройки коллекции перейдите на вкладку “**Session**” и выставите следующие настройки:

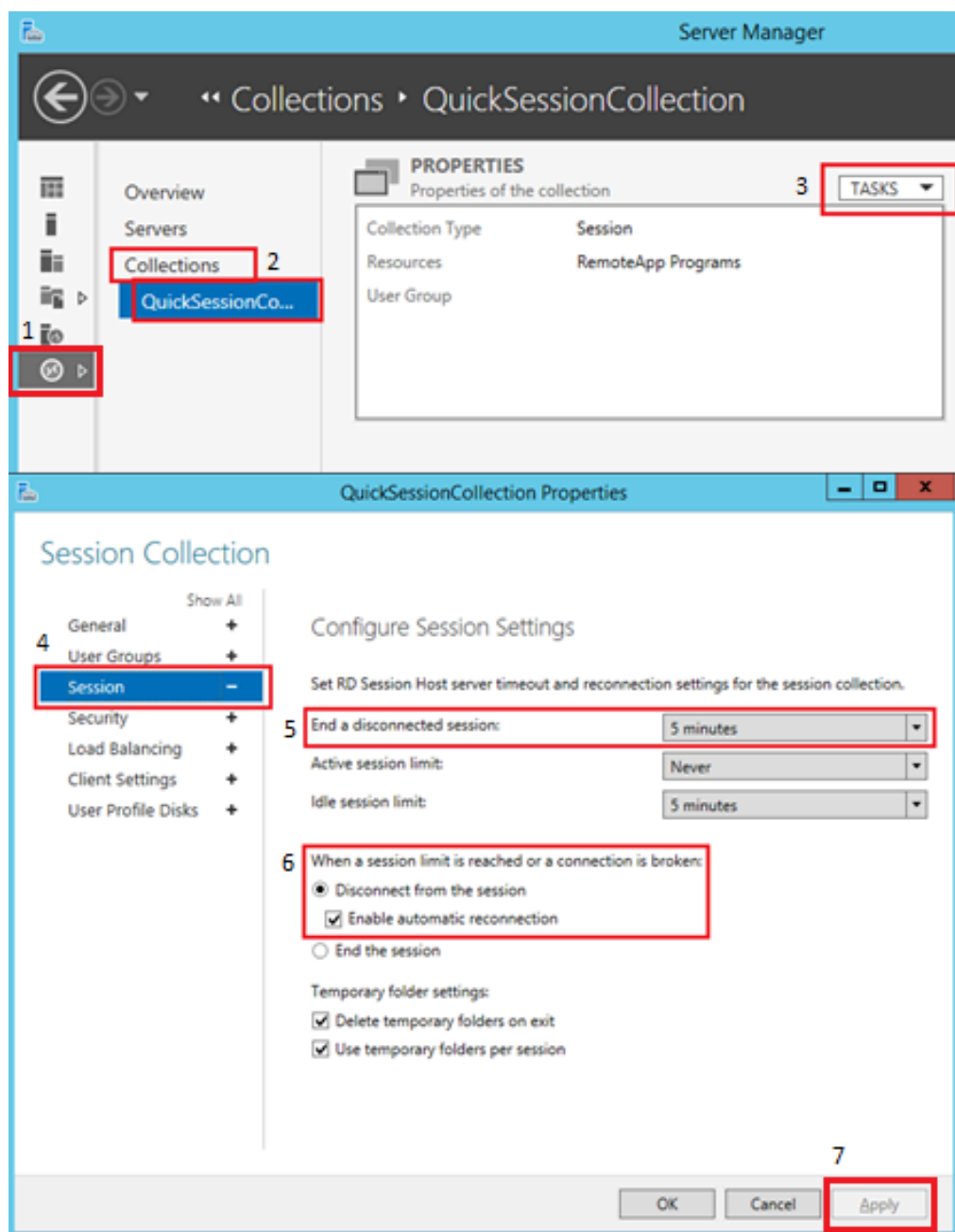


Рис. 23. Настройка коллекции

Обязательная настройка:

“End a disconnected session”: 5 minutes (рекомендуемое значение: от 1-ой до 5-ти минут).

Рекомендуемая настройка:

“When a session limit is reached or a connection is broken”:
Disconnect from the session (Enable automatic reconnection).

5. Подтвердите изменения, нажав на кнопку **“Apply”**. Убедитесь, что настройки были успешно сохранены. Далее закройте окно, нажав на **“OK”**.

6. Теперь в разделе **“RemoteApp Programs”** нажмите на кнопку **“TASKS”** и в выпадающем меню выберите **“Publish RemoteApp Programs”**.

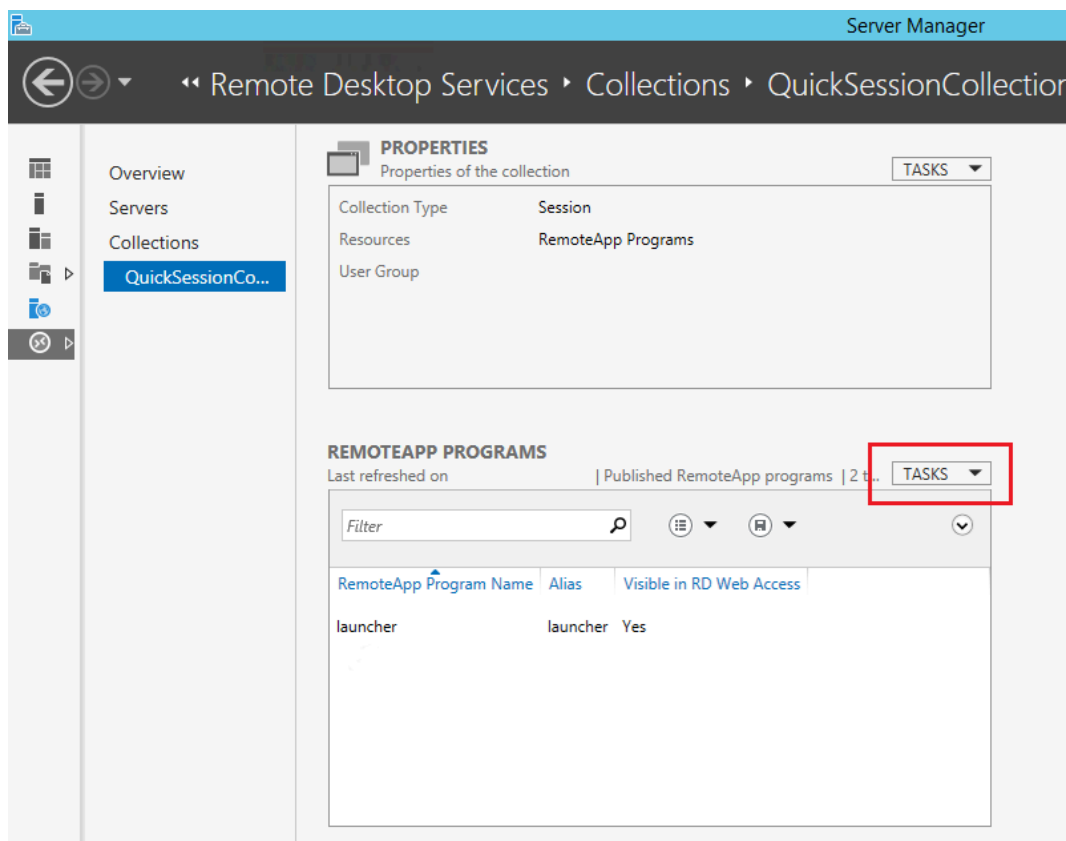


Рис. 24. Публикация нового RemoteApp

После открытия мастера публикации RemoteApp выполните следующие шаги:

7. Нажмите кнопку **“Add”** для добавления нового приложения.
8. Выберите компонент **“launcher.exe”**, он будет находиться в каталоге, созданном при развертывании служб управления и мониторинга процессами, по адресу: **C:\space\space-Jump-Server\ec\launcher.exe**
9. Нажмите кнопку **“Open”** для добавления приложения в список.
10. Выберите добавленное приложение и нажмите **“Next”**.
11. На следующем экране мастера публикации RemoteApp нажмите кнопку **“Publish”**.

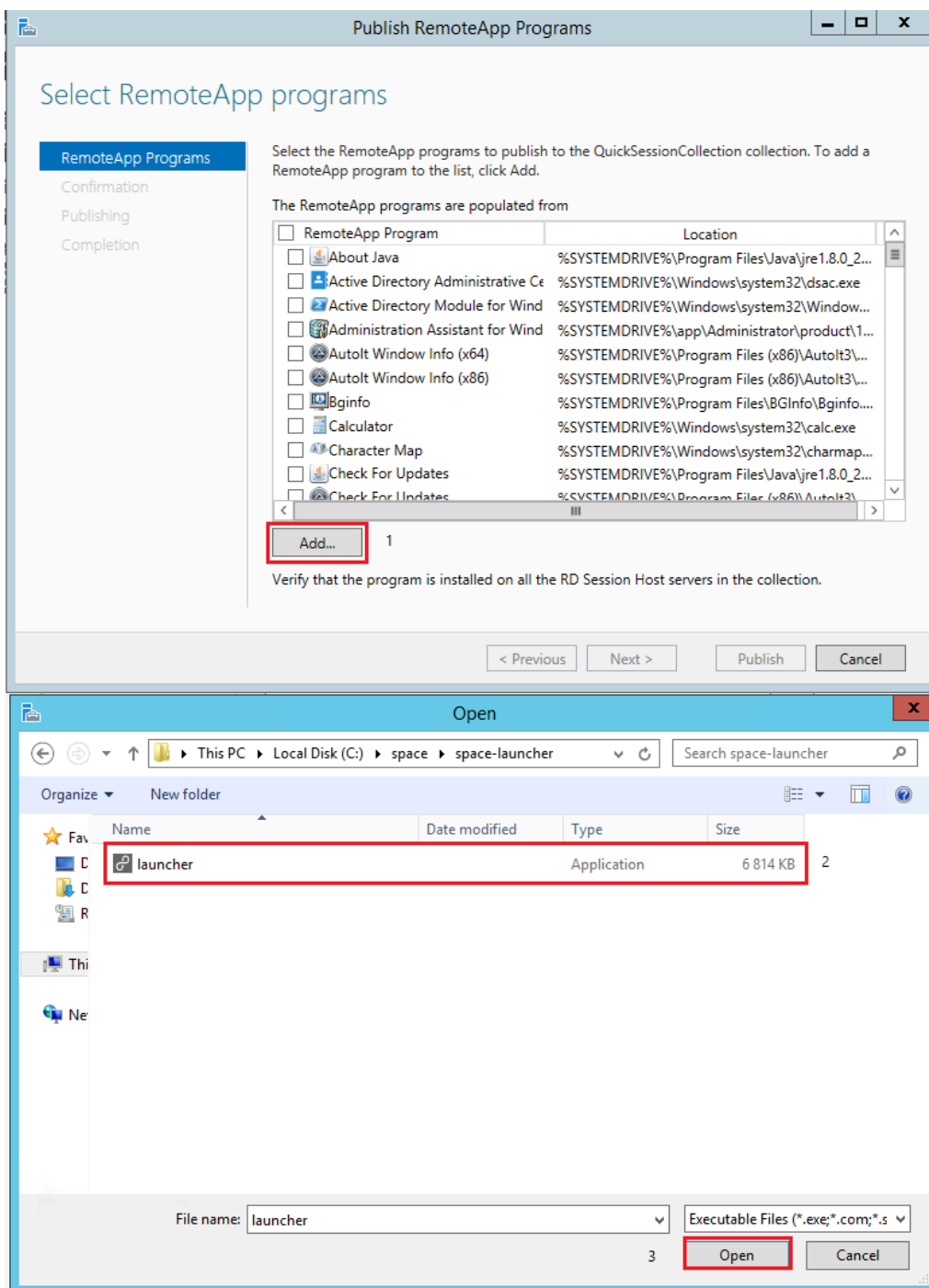


Рис. 25. Добавление нового приложения

После публикации нового RemoteApp перейдите в его контекстное меню и выберите **“Edit Properties”**.

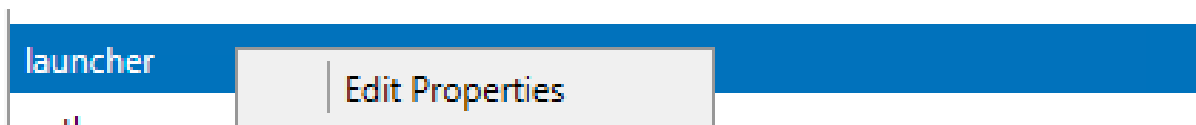


Рис. 26. Контекстное меню

Следом откроется окно **“Properties”**. После чего необходимо выполнить следующие шаги:

12. Перейти в раздел **“Parameters”**.
13. Выбрать режим **“Allow any command-line parameters”**.
14. Нажать кнопку **“Apply”**.

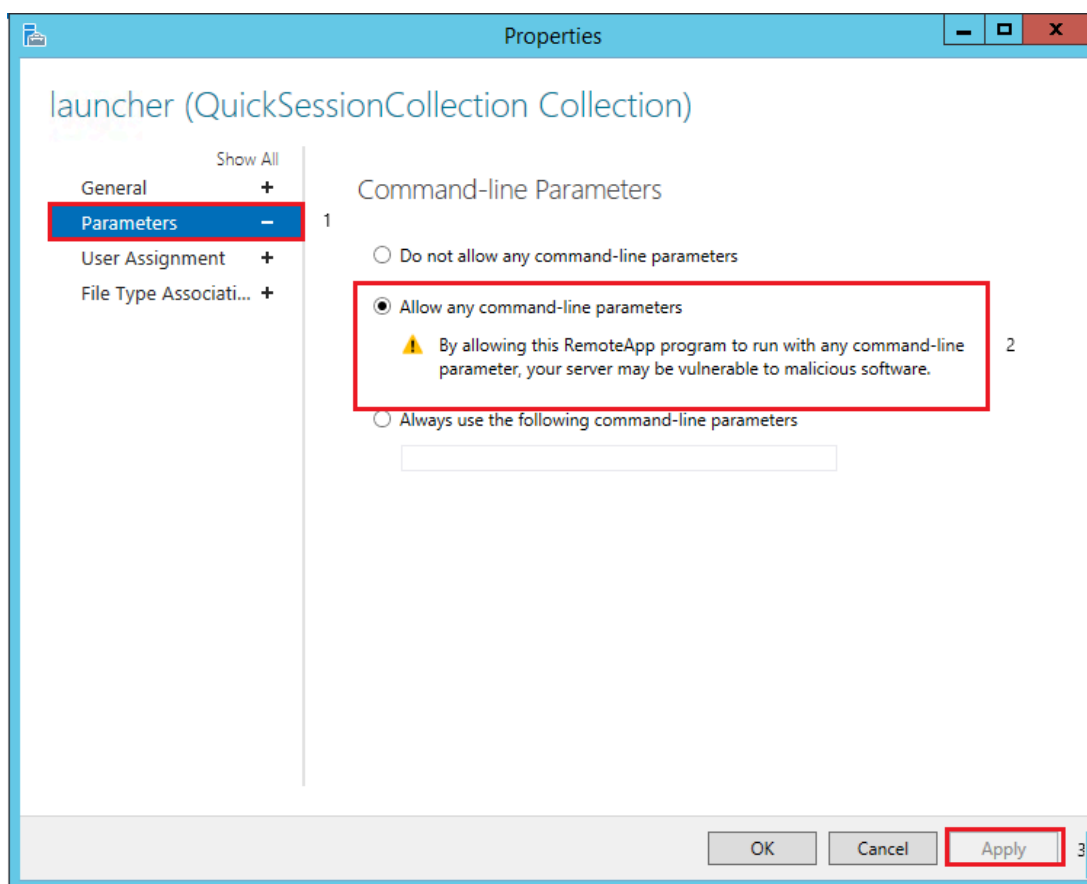


Рис. 27. Выбор режима для приложения

5.7.3. Рекомендации для ЗСА Windows

В качестве рекомендации по ограничению доступа для рядовых пользователей на сервер запуска приложений системы sPACE можем предложить два варианта:

- замену запуска стандартного Shell в операционной системе Windows на другое приложение;
- запрет запуска explorer.exe настройками доступа для всех, кроме локальных администраторов сервера СЗС.

Основной вариант

В примере ниже используется запуск инструмента «Ножницы». В качестве приложения нужно выбрать существующий на сервере и являющийся исполняемым файл (например logoff.exe).

Для настройки вам потребуется запустить на сервере запуск приложений консоль mmc и открыть добавление инструментов.

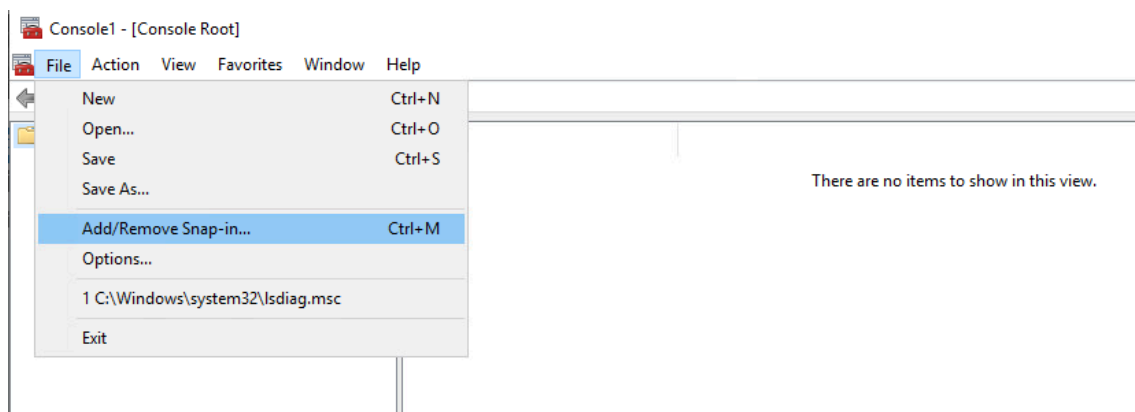


Рис. 37. Добавление инструментов

Далее вы выбираете из списка нужную политику.

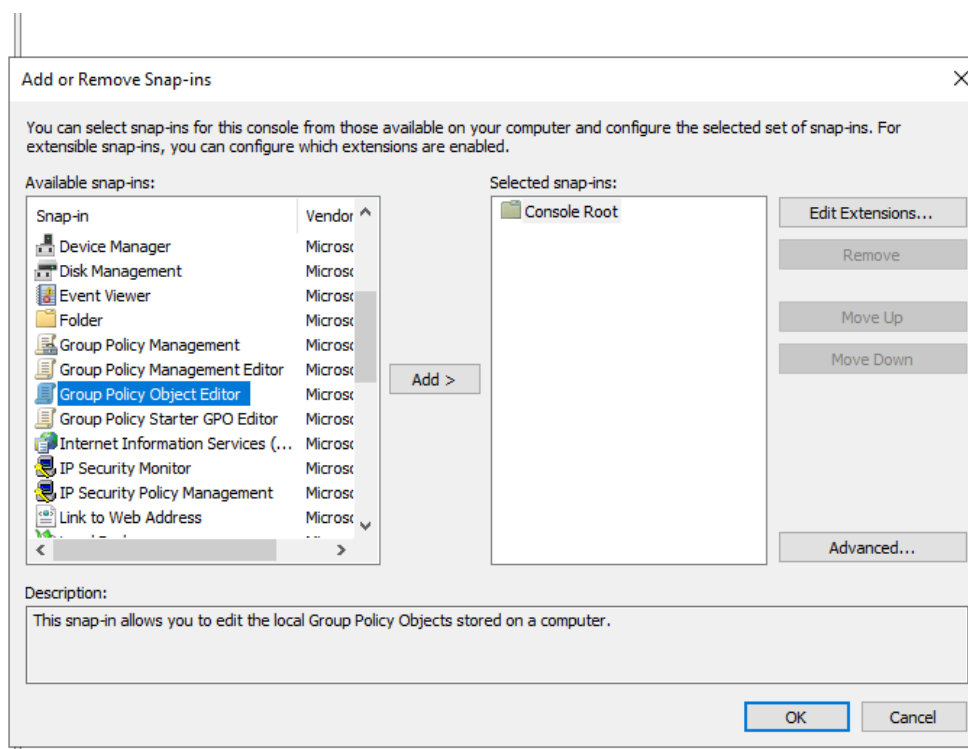


Рис. 38. Добавление групповой политики

После добавления политики выбираете «обзор» и в открывшемся окне выбираете нужный список пользователей (в нашем случае это условие «не администраторы»).

Welcome to the Group Policy Wizard



Local Group Policy Objects are stored on the local computer.

Use the Browse button to select one of the Group Policy Objects.

Group Policy Object:

Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This only applies if you save the console.

< Back Cancel

Welcome to the Group Policy Wizard



Browse for a Group Policy Object ? ✕

Computers Users

Local Users and Groups compatible with Local Group Policy:

Name	Group Policy Object Exists
Administrator	No
ADMIN_IHELP21RU	No
DefaultAccount	No
WDAGUtilityAccount	No
Administrators	No
Non-Administrators	Yes

Рис. 39. Выбор списка пользователей

После добавления открываем политику в разделе, показанном на скрине ниже.

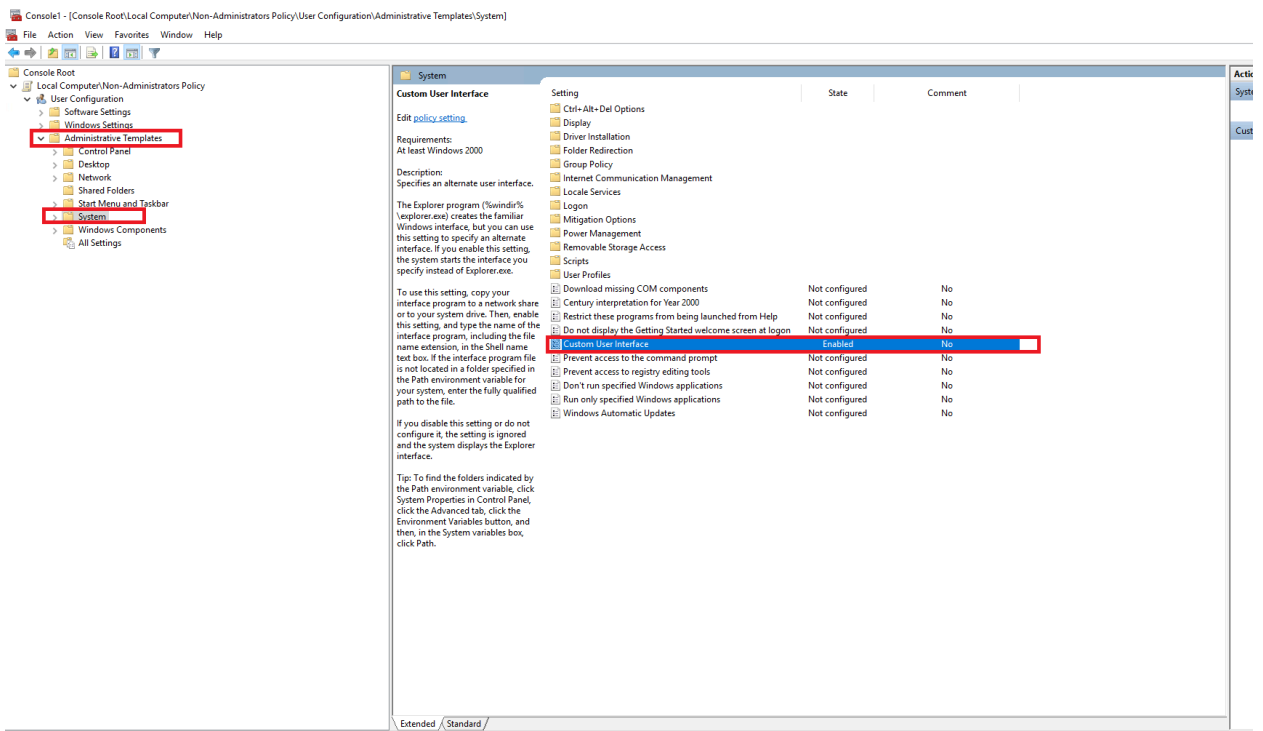


Рис. 40. Открытие политики в разделе

Меняем значение данной настройки на любой исполняемый файл, применяем политику и перезагружаем сервер.

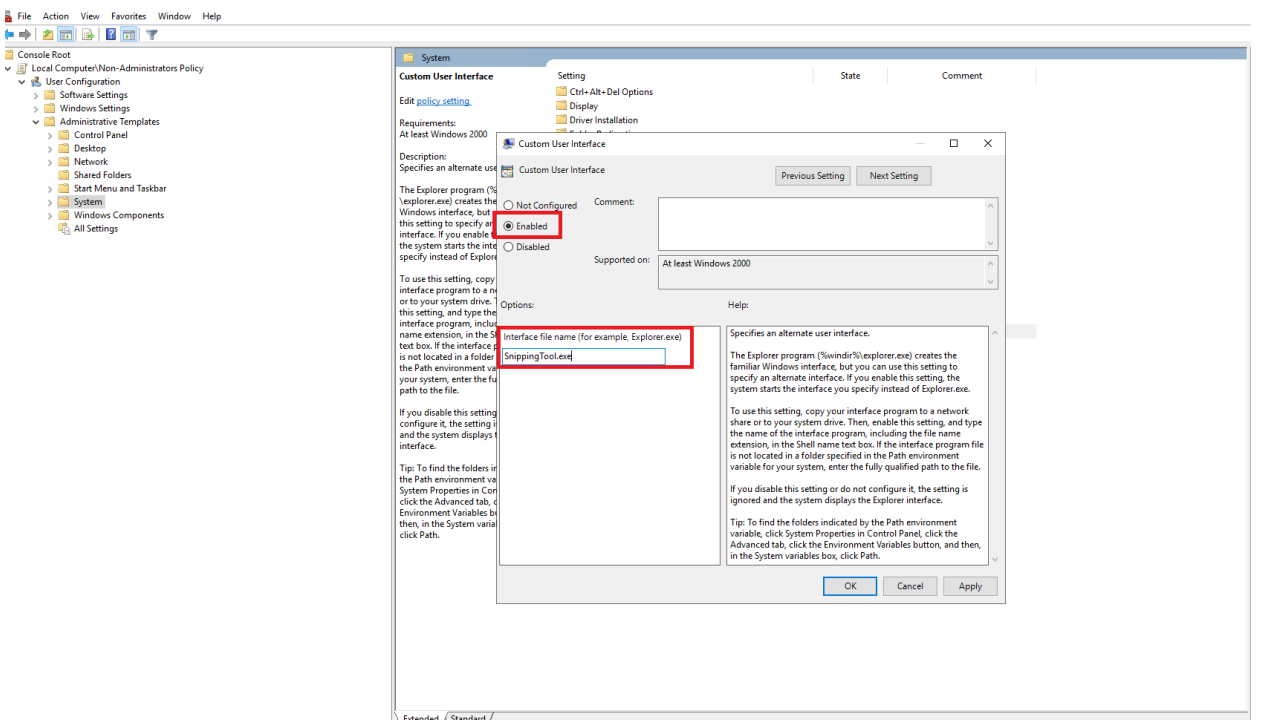


Рис. 41. Изменение значения настройки

В результате администраторы сервера (те, что входят в локальную группу администраторов) смогут зайти на сервер в обычном режиме, а пользователи не смогут осуществлять работу с сервером при прямом RDP подключении. На работу системы SPACE данная настройка не влияет.

Альтернативный вариант

Второй вариант ограничения доступа более жесткий – запрет запуска explorer.exe настройками доступа для всех кроме локальных администраторов сервера ЗСЗ.

C:\Windows\ → находим файл explorer.exe → ПКМ → Свойства → Безопасность → Дополнительно → Меняем владельца с TrustedInstaller на <Admin>

Применяем и сохраняем настройки нажатием на Apply и ОК. Снова:

ПКМ → Свойства → Изменить → Выбираем пользователя, у которого надо убрать разрешение на запуск Explorer → Снимаем галочки с "Чтение и выполнение", "Чтение"

На скрине ниже пример настройки.

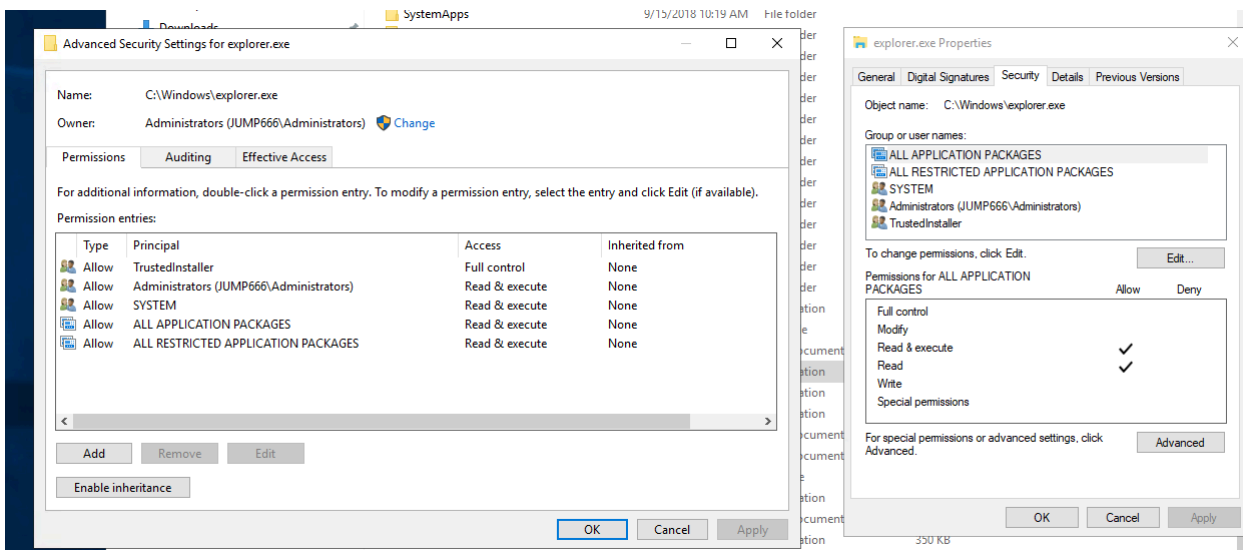


Рис. 42. Альтернативный жесткий вариант ограничения доступа

5.8 Настройка групповых политик ЗСА Windows

Откройте инструмент **Group Policy Management** для того домена, в котором располагаются сервера ЗСА:

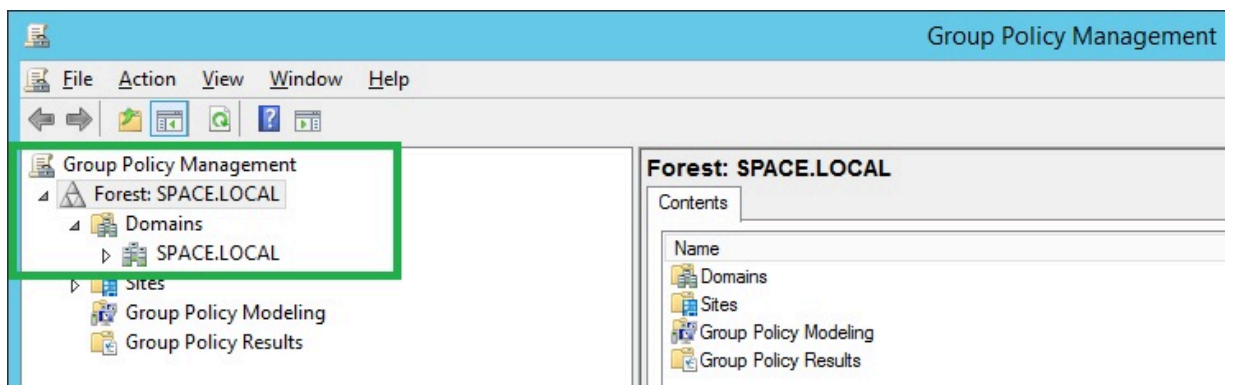


Рис. 28. Group Policy Management – управление групповыми политиками в домене

5.8.1 Настройка соединений RDS

1. В контекстном меню выберите действие для создания объекта групповой политики домена:

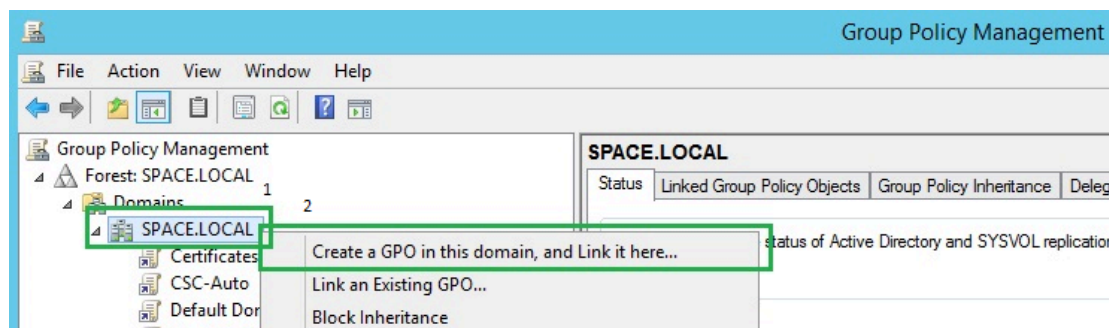


Рис. 29. Group Policy Management – создание объекта групповой политики

2. Задайте удобное имя, отражающее суть настроек в данном объекте, и нажмите “OK”. Например, для данного пункта: “**Connections Settings**”:

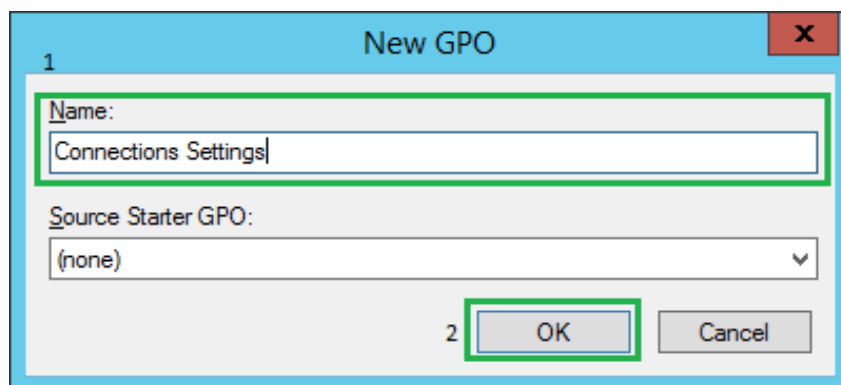


Рис. 30. Group Policy Management – имя объекта групповой политики

3. В списке объектов групповых политик выберите вновь созданный объект и откройте окно его редактирования, выбрав в контекстном меню **“Edit...”**:

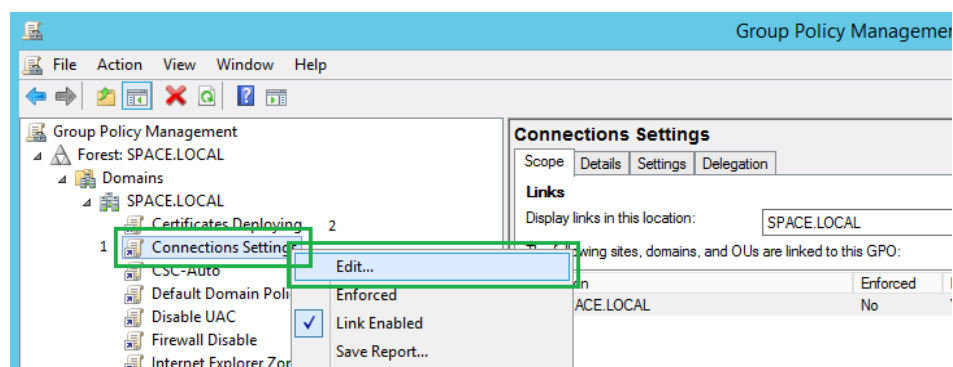


Рис. 31. Group Policy Management – открытие окна редактирования объекта групповых политик

4. В левом дереве выберите следующий раздел настроек:

“Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections”:

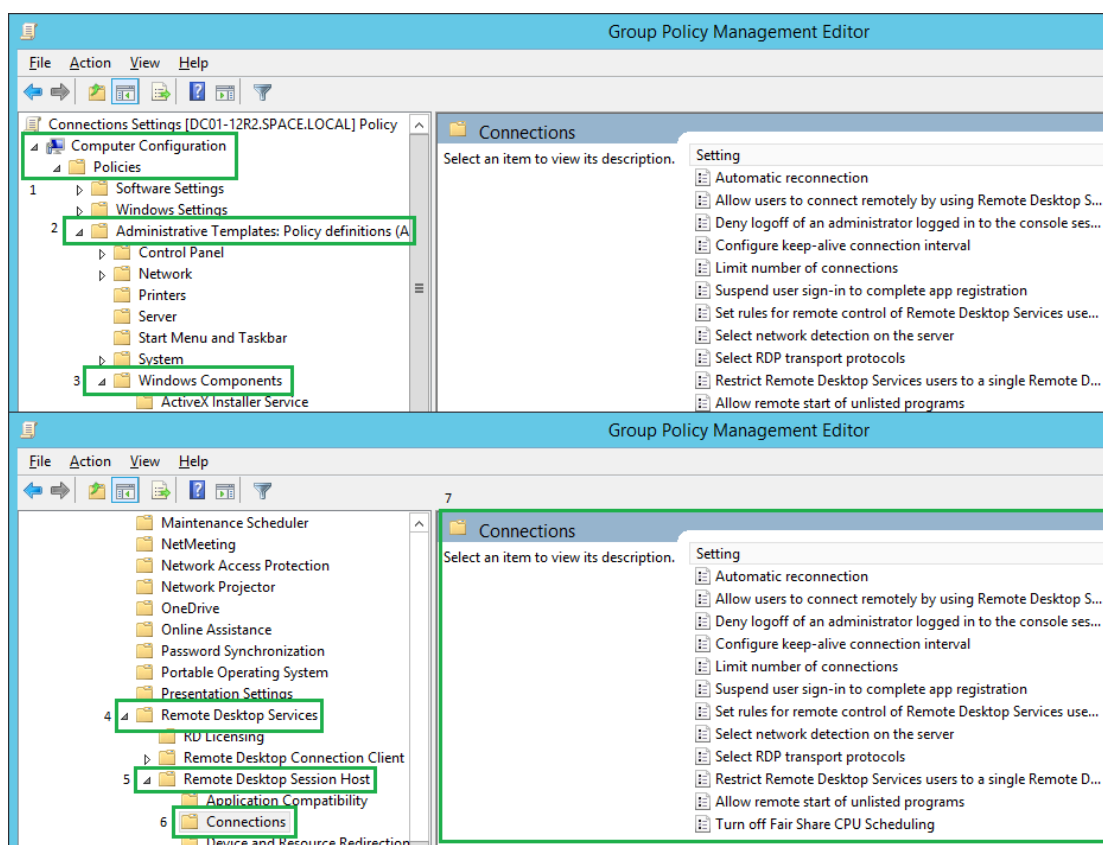


Рис. 32. Group Policy Management – выбор раздела настроек

5. Перейдите в режим редактирования настройки **“Limit number of connections”** путем двойного нажатия или выбрав редактирование в контекстном меню:

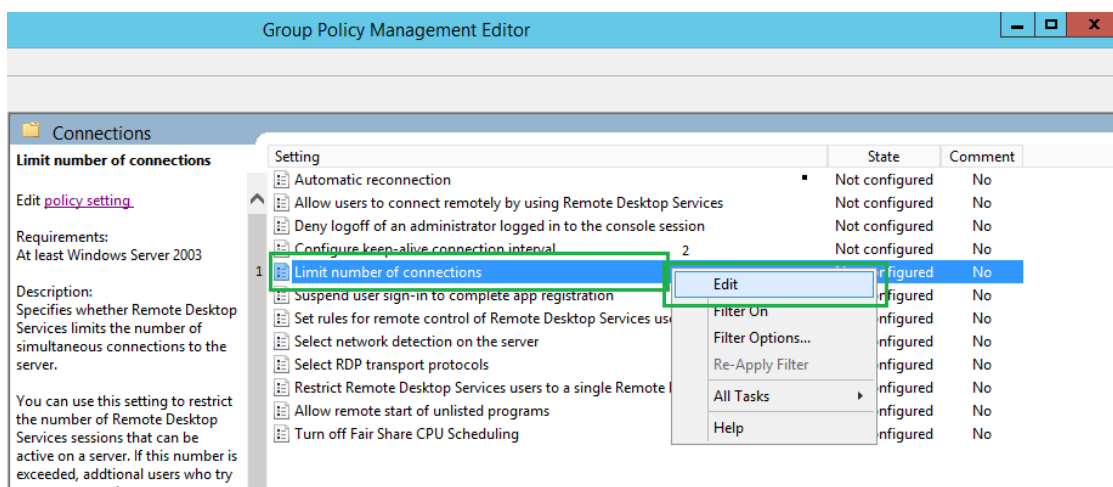


Рис. 33. Group Policy Management – переход в режим редактирования настройки

6. Включите данную настройку, установите значение в **“999999”** для неограниченного числа подключений и сохраните изменения:

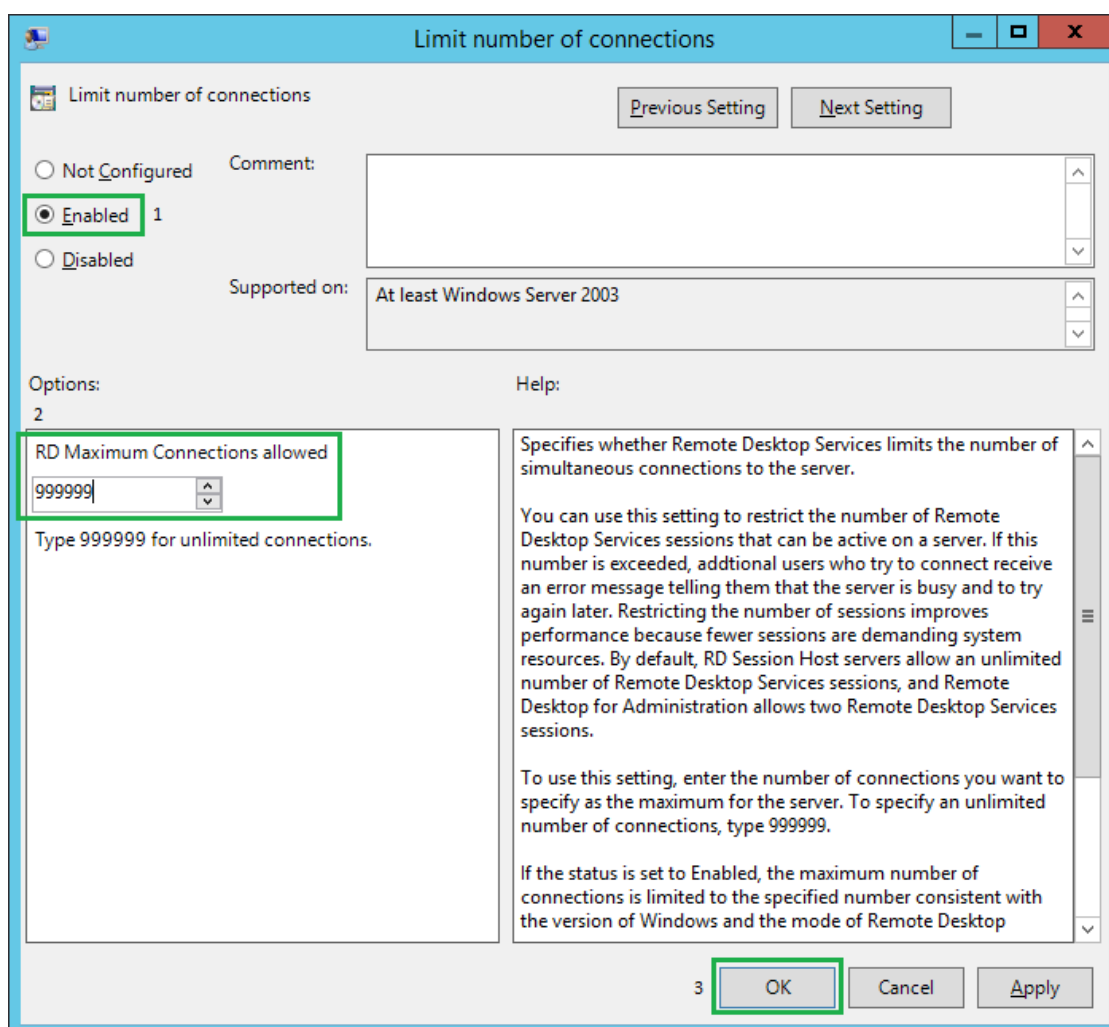


Рис. 34. Group Policy Management – редактирование настройки ограничения числа подключений

7. Теперь перейдите в настройку **“Restrict Remote Desktop Services users to a single Remote Desktop Services session”** и отключите её, выбрав **“Disabled”**:

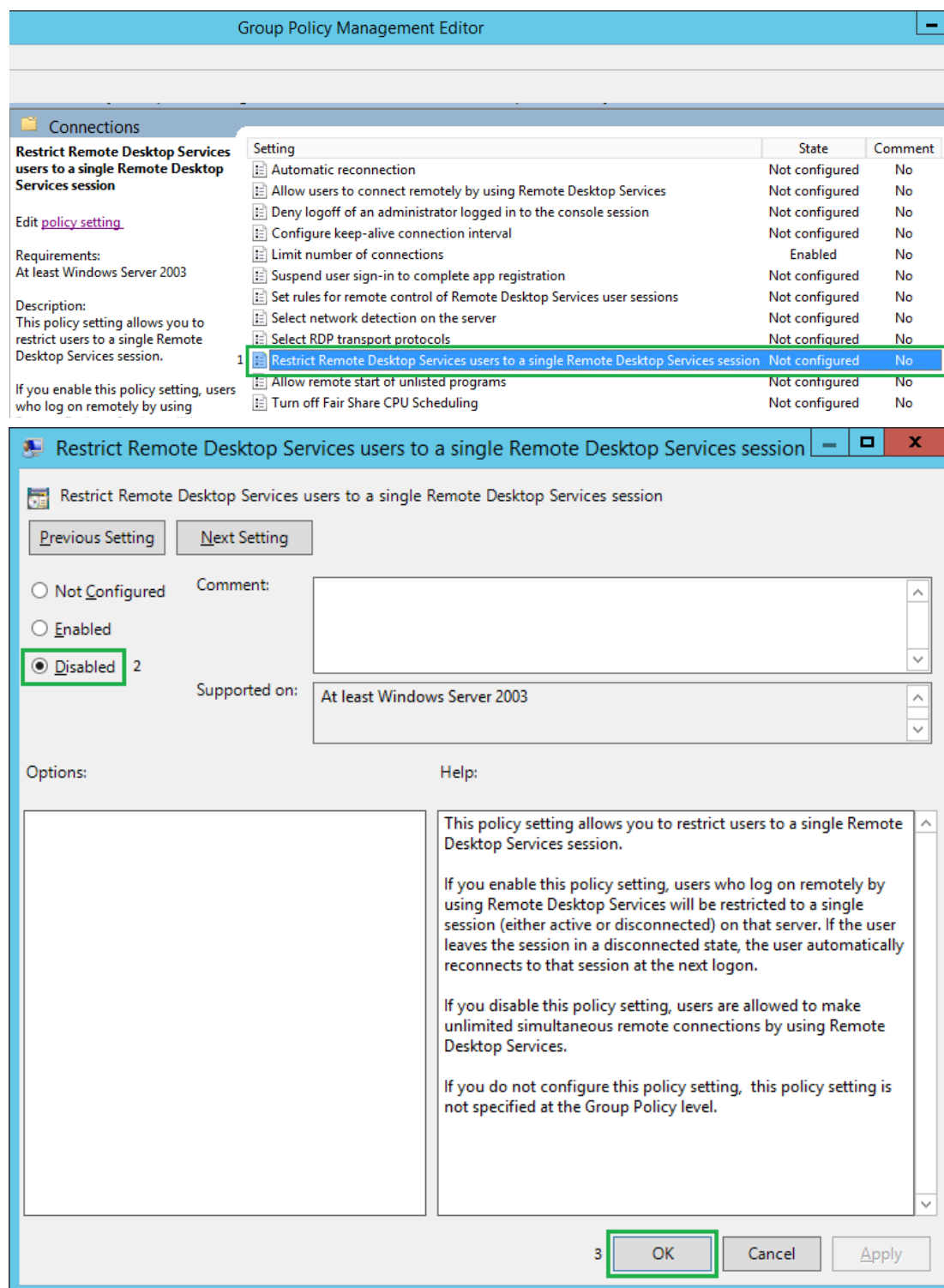


Рис. 35. Group Policy Management – редактирование настройки

Первоначальная настройка СУПД sPACE PAM завершена! Теперь вы можете воспользоваться руководством пользователя и руководством администратора, в которых описаны основные принципы работы sPACE PAM, а также добавление остальных элементов системы и запуск сеансов.

6. Настройка отказоустойчивой системы

6.1. Схема отказоустойчивой системы

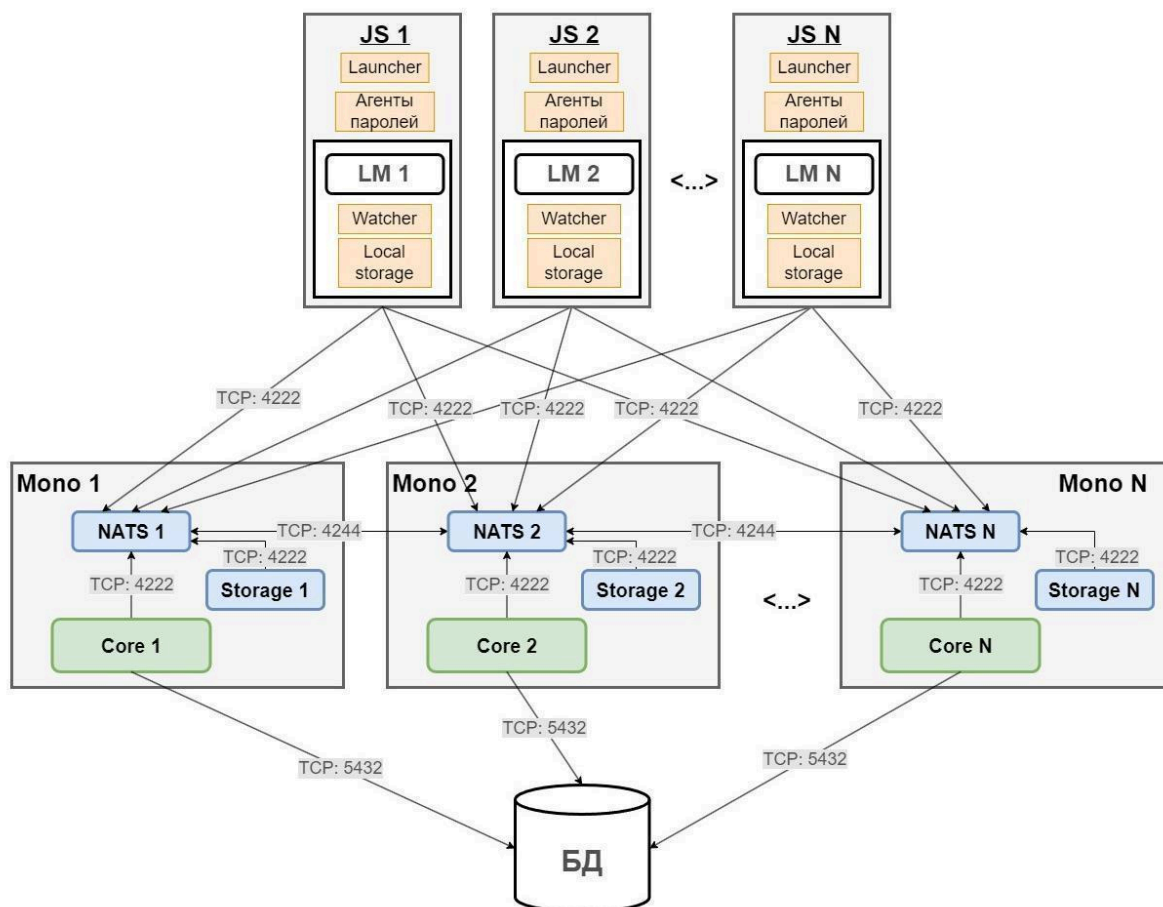


Рис. 36. Отказоустойчивая система с N Ядрами.

Обозначение элементов схемы:

JS – Защищенная Среда Администрирования.

LM – Launch Manager для запуска сеансов.

TCP – информация о протоколе, порте и направлении соединения.

Mono – кластер NATS.

Storage – Хранилище видео.

Core – Ядра системы.

БД – сервер PostgreSQL.

6.2. Процесс установки второго (или N-го) Ядра системы

1. Загрузить установочный файл на новое ядро в соответствии с пунктами 1-4 раздела 5.1 данной инструкции (Установка на Linux).

2. Запустить выполнение файла в тихом режиме при помощи команды “sh spaceinstall-2.0.2.5744 IP-адрес_машины_с_инсталляцией_ядра space-api пароль_space-api пароль_root_машины_установки

Пример: sh spaceinstall-2.0.2.5744 192.168.74.193 space-api space-api Zaq12wsx

Примечание: В дальнейшем, при обновлении отказоустойчивой конфигурации, второе (или N-е) ядро обновляется путем запуска файла в обычном режиме при помощи команды:

sh полное_имя_файла (Пример: sh spaceinstall-2.0.2.5744)

3. Установка отказоустойчивой системы в тихом режиме занимает около 5-10 минут.

4. На данном этапе примерно через 10 минут в интерфейсе sPACE на обоих Ядрах в разделе «**Управление ресурсами**» > «**Статус компонентов**» на вкладке «**Ядра системы**» должны появиться оба Ядра.

5. Проверить работоспособность второго (или N-го) ядра портала sPACE.

Примечание: при обновлении отказоустойчивой системы нужно останавливать второе ядро (или последующее N-ое число ядер).

7. Список стороннего ПО

Таблица 10. Список стороннего ПО

ПО	Описание	
JRE	Java SE Runtime Environment (x64)	
JCE	Java Cryptography Extension	
PostgreSQL DB	База данных PostgreSQL	страница загрузки
Tomcat	Контейнер сервлетов (x64)	страница загрузки
NATS	Платформа, реализующая систему обмена сообщениями (COC)	страница загрузки
AutoIt	Скрипт для автоматизации выполнения задач в ОС Microsoft Windows.	страница загрузки
Docker CE	Система контейнеров для Linux.	страница загрузки

Приложение 1: Чек-лист подготовки инфраструктуры

- o **Программное обеспечение на Сервер sPACE Mono (Base):**
 - o Одна из ОС: CentOS 7-8, Ubuntu 22.04 и 24.04, Astra Linux «Орёл», Red OS «Муром» 7.3.2, ALT Linux 10;
 - o Файловая система ОС не находится в режиме **Read-only**;
 - o Установлен OpenSSL 1.1.1 и выше;
 - o Запущен Docker 24.0 и выше;
 - o Установлен Wget (GNU Wget);
 - o Установлен tar (tape archive);
 - o Установлен awk;
 - o Установлен sed (Stream Editor).
- o **Программное обеспечение на Сервер ЗСА Windows:**
 - o Microsoft Windows Server 2012-2019;
 - o Remote Desktop Server (RDS) (Службы удаленных рабочих столов):
 - Remote Desktop Session Host (Узел сеансов удаленных рабочих столов);
 - Remote Desktop Connection Broker (Посредник подключений к удаленному рабочему столу);
 - o Установлен Windows PowerShell 5.1 и выше.
- o **Программное обеспечение на Сервер ЗСА Linux (SSH):**
 - o Одна из ОС: CentOS 7-8, Ubuntu 22.04 и 24.04, Astra Linux «Орёл», Red OS «Муром» 7.3.2, ALT Linux 10;
 - o Установлен OpenSSL 1.1.1 и выше;
 - o Запущен Docker 24.0 и выше;
 - o Установлен Expect;
 - o Установлен Wget (GNU Wget);
 - o Установлен unzip;
 - o Установлен SSH (Secure Shell).
- o **Программное обеспечение на Сервер ЗСА Linux (RDP):**
 - o ОС ALT Linux 10;
 - o Установлен OpenSSL 1.1.1 и выше;
 - o Запущен Docker 24.0 и выше;
 - o Установлен Expect;
 - o Установлен Wget (GNU Wget);
 - o Установлен unzip;
 - o Установлен SSH (Secure Shell).
- o Выполнены все условия пункта 3.5 «**Требования к инфраструктуре**» из инструкции по развертыванию;
- o Обеспечена сетевая доступность - открыты порты из таблицы 7 «**Список требуемых к открытию сетевых портов**» из инструкции по развертыванию.