ООО «ВЭБ КОНТРОЛ ДК»



# Система Управления Привилегированным Доступом sPACE PAM

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 РАМ	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 РАМ	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 3CA Windows	24
5.7.3. Рекомендации для 3CA Windows	28
5.8 Настройка групповых политик 3CA 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:

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.
OA	Объект Администрирования — целевая система, где производятся административные действия.
<b>ЗСА</b> (или <b>СЗС</b> )	Защищенная Среда Администрирования (или Сервер Защищенной Среды) — выделенный сервер, на котором выполняется сеанс администрирования.
ИА	Инструмент Администрирования — приложение, запускаемое на сервере <b>ЗСА</b> , с помощью которого осуществляются административные действия в <b>ОА</b> .
сос	Служба Обмена Сообщениями — служба, обеспечивающая коммуникацию между компонентами СУПД.

Таблица 1 «Термины и сокращения»

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 OA. 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* OC 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»

Состав ПО
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).
Microsoft Windows Server 2012-2019;
Remote Desktop Server (RDS);
Windows PowerShell 5.1 и выше.
CentOS 7-8, Ubuntu 22.04 и 24.04, Astra Linux «Орёл», Red OS «Муром» 7.3.2, ALT Linux 10;
Примечание: для запуска на СЗС Linux приложений с графической оболочкой поддерживается только ALT Linux.
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)	ЗГБ
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 1024х768 и больше (рекомендуется 1920х1080), 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.
Привилегированны й 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 3CA 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	Рабочие 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:

- Установку 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 3CA (пункт «5.5 Установка сервера 3CA»). Также нельзя пренебрегать промежуточными пунктами установки (5.2-5.4), особенно если вы 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 сервер Windows под развертывание 3CA Windows установлен Remote Desktop Services с установленными Collection.
- Сервер Windows под развертывание 3CA 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 3CA Windows установлена версия PowerShell не ниже 5.1.14409.1029.
- На сервере Linux под развертывание 3CA Linux установлен инструмент автоматизации Expect и пакет Openssl не ниже версии 1.1.
- На сервере Linux под развертывание sPACE Mono и на сервере 3CA 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 3CA Linux (работа приложения с графической оболочкой), то на нём должны быть заранее установлены пакеты xorg-server-common, xrdp и dwm. Также такой 3CA 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.



вас приветствует мастер установки к Проверьте настройки таймзоны!	COMICHENTOB CNCTEMM SPACE.
Текущая таймзона: Europe/Moscow	
Если эта таймзона отличается от Вашей, выйдите из установщика, и настройте на сервере правильную таймзону. Если всё в порядке, выберите "Далее". После нажатия Enter начнётся установка sPACE.	
Для выхода выберите "Отмена".	
<Далее>	<Отмена>

Рис. 3. Начало установки

9. Начнётся процесс установки.

Распаковка временных файтов
10%
Создание структуры базы данных
518

Установка	Storage		
		80%	

#### 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.

Установка завершена	!
20122	

Рис. 5. Завершение установки

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

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

[root@te CONTAINI 862a43aa 04c73e3 a822c29 6f08964	estmono ER ID a1863 2643e 59c29 ef2b5	<pre>redos spaceinstall]# do IMAGE tomcat:8.5-jdk8 space/storagebuntu:1 nats postgres:9.6</pre>	cker ps COMMAND "catalina.sh run" "/var/opt/space/ec/s" "/nats-serverconf" "docker-entrypoint.s"	CREATED 3 minutes ago 3 minutes ago 4 minutes ago 11 minutes ago	STATUS Up 3 minutes Up 31 seconds Up 3 minutes Up 11 minutes	PORTS	NAMES spacetomcat8 spacestorage nats-server spacepostgres9
STA	TUS	3		]	PORTS	NAMES	
Up	Зn	ainutes				spacetom	icat8
Up	31	seconds				spacesto	rage
Up	3 n	ainutes				nats-ser	ver
Up	11	minutes				spacepos	tgres9

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 <u>https://IP или DNS имя ядра</u>.

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**».

Bace		•
		-
	Тенант:пользователь@домен	
	Пароль	
	Считать пароль с ТМ      ⊕ Русский •	
	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».

🕱 Поиск по навигации	
Управление ресурсами	
Пользователи	
— 🖬 Интерпретаторы	
— 🖬 Приложения	
—∎ Серверы ЗС	

Рис. 8. Местонахождение раздела «Пользователи» в системе

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

	Статус компонентов × Лице Добавить Удалить	нзия 🗙 ручетные записи Отключить поддержк	× Список пользователе	u x
	Имя пользователя	Домен	ФИО	
вания	admin 📃	internal		

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 «space-api»), **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				:	N
Имя пользователя :	space-api	Ð	Тенант :	main 🗸 🗸	
Фамилия :		0	Мобильный телефон :	0	
: кмИ		0	Телефон :	0	
Отчество :		0	Электронный адрес :	0	3
Пароль :	•••••	Ð	Роли :	ROLE_API_MANAGEM ×	8
Подтверждение пароля :	•••••	Ð	l	Введите значения	2
Требования :	Длина пароля: 6; содержит строчные и прописные буквы; содержит цифры			· ·	
	Ограничить				ž.
				, <b>A</b>	9
	Ż	R	) * *		
Сохранить Сгененр пар	оировать Показать\скрыть роль 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.

😗 Поиск по навигации	Список пользователей 🗙				🥚 admin 🛛 🚊 🗸
Ф Управление системой	Добавить Удалить	Отключить поддержку 2FA			Загр 🗿 Настройки
Управление ресурсами					Отрофиль     Отрофиль     Отрофиль
🗃 Тенанты	Имя пользователя	Тенант	ΦΝΟ	Роли	2FA Ø О программе
- 🖿 Пользователи	example	main		ROLE_SPACE_ADMIN, ROLE_SPA	С Выход
🖬 Интерпретаторы	🔲 admin	main		ROLE_API_MANAGEMENT, ROLE	
— 🖬 Приложения					
— 🖬 Серверы ЗС					
пользовательские роли					
Системные настройки					
<ul> <li>— Журнал сооытии</li> <li>Виляериний видеоридит</li> </ul>					
Внутренний видеоаудит					
н- Статистика					
		3arp	Настройки Профиль Справка О программе Выход		

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 ЗС» должно гореть красным, поскольку серверы ЗС еще не были установлены.



		Экспортировать Развернуть
		``
aı	IME	нование
•		Основные
•		Ядра системы
		Сервера ЗС
		Agpeca DNS
		Контроллеры домена
•	Ē	Сервера системы доставки сообщений
	Ô	Разница в системном времени компонентов системы
	Ô	Состояние Хранилищ ВСАС

Рис. 16. Вкладка «Статус компонентов»

#### 5.5 Установка сервера ЗСА

Сервер ЗСА может быть представлен на машине Windows или Linux.

#### 5.5.1 Сервер 3CA 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 3CA 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.

	4		
		Open	
space	9	Run as administrator	
er- 1.4. e		Troubleshoot compatibility	
		Pin to Start	
	È	Share	
		Give access to >	
		Pin to taskbar	
		Restore previous versions	
		Send to $>$	
		Cut	
		Сору	
		Create shortcut	
		Delete	
		Rename	
		Properties	



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 C3C Windows завершена! Далее перейти к установке C3C Linux (при необходимости) или пункту введения сервера 3C в используемые в веб-интерфейсе.

6. В дальнейшем, при обновлении сервера 3CA 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 3CA 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 3CA 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 3CA, 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@jsalttest 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 СЗС Linux завершена! Далее перейти к пункту введения сервера ЗСА в балансировку.

5. В дальнейшем, при обновлении сервера 3CA 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.

Поиск по навигации	Список пользователей 🗙 Серверы ЗС 🗙			😑 admin 🛛 🚊 루
Ф Управление системой	Используемые Серверы ЗС			
Управление ресурсами	Добавить Удалить Задать Внешний	D		Загружено: 0 🔗
Пользователи				9
	🔳 Имя FQDN	Доступен	Терм. соединения	Сессии
<ul> <li>Сорене и О</li> <li>Пользовательский роли</li> <li>Системные настроки</li> <li>Журнал событий</li> <li>Внутрений видоозудит</li> <li>Статус компонентов</li> <li>Лицензия</li> <li>Статистика</li> </ul>	Неиспользуемые Серверы 3С	Нег объектов для вывода.	A	
$\lambda$	Добавить Удалить Задать Внешний	D		Загружено: 2 Всего записей: 2 🔘
$\lambda$				
A A A A A A A A A A A A A A A A A A A	Имя	FQDN		Доступен
*	is2.demo.lab	js2.demo.lab		
	ps.demo.au	js.œmo.iap		

Рис. 19. Введение сервера ЗС в используемые

2. Подтвердить ввод сервера ЗСА в используемые.



Рис. 20. Пример добавления сервера 3С 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 3С. Для этого нужно нажать на него в таблице серверов, открыть карточку и удостовериться, что прописан верный тип подключения.

Сервер ЗС	como fado addross			×
Имя:	test-domain-name-2216	FQDN :	some-fqsn	0
Домен :	test-domain-2216-1 ·	Тип подключения :	RDP •	0,
Тип ОС :	Windows 🗸	Система видеоаудита :	ВСАС × Введите значения •	0
Внешний ID :	some-jump-server-id-2216	B RD gateway :		<b>0</b> .
Создан :	03.05.2023 16:30:21	Изменен :	09.01.2024 12:41:15	? X
Прос	смотр Сохранить	Закрыть .		

Рис. 21. Пример добавления сервера 3C Windows

**Примечание:** тип подключения выбирается на основе того, каким будут запускаемые на данном C3C сеансы.

- Если это будут сеансы с графической оболочкой, то нужно выбирать тип подключения RDP независимо от того, является ли сервер 3C 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 ceaнca.

Тип сервера ЗС	Тип подключения	Тип рабочей машины пользователя	Файл подключения
Windows	RDP	Windows	RDP файл для C3C Windows
Linux	RDP	Windows	RDP файл для C3C Linux
Windows	RDP	Linux	Строка XfreeRdp для C3C Windows
Linux	RDP	Linux	Строка XfreeRdp для C3C 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	іса файл
Linux	Citrix	Windows, Linux	_

**Примечание:** если нужен сервер 3C 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 3C (см. картинки ниже).

Сервер ЗС				×
Имя :	t1ljs01.spacetest201.lab	0	FQDN :	t1ljs01.spacetest201.lab
Тенант :	~	0	Тип подключения :	SSH × RDP × 0 Введите значения •
Тип ОС :	Linux ~	0	Система видеоаудита :	ВСАС Х Введите значения С
Внешний ID :	d298e5b2-3405-4d86-bf52-87	0	RD gateway :	0
Создан :	28.08.2024 17:14:39		Изменен :	12.12.2024 13:00:18
Прос	смотр Сохранить	ļ	Закрыть	

Рис. 22. Сервер 3С, поддерживающий два типа подключения

Далее требуется только настроить Объекты администрирования. Приложения с графической оболочкой должны запускаться на сервере 3С с подключением RDP, а приложения без графической оболочки — на сервере 3С с подключением SSH.

# 5.7 Дополнительная настройка для сервера 3CA Windows 5.7.1 Настройка приложений

Для того чтобы в Системе работал запуск приложений, используемых в сценариях, соответствующие приложения должны быть установлены на сервере 3С. 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 3C 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:

řa –		Server Manager
<b>€</b> ∋• "Co	llections • QuickSessionColle	ection
Overview Servers Collections QuickSessionCo	2 PROPERTIES Properties of the collection Collection Type Session Resources RemoteApp I User Group	3 TASKS -
Session Collection Show All General + User Groups + Session -	Configure Session Settings Set RD Session Host server timeout and reconnection	settings for the session collection.
Security + Load Balancing + Client Settings + User Profile Disks +	5       End a disconnected session:         Active session limit:         Idle session limit:         Idle session limit is reached or a connection is browned by Disconnect from the session         Image: Disconnect from the session <th>5 minutes</th>	5 minutes
		7

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**".

è		Se	rver Manager
$\mathbf{E}$	. • Remot	e Desktop Services • Collections • QuickSe	essionCollectior
	Overview Servers Collections QuickSessionCo	PROPERTIES         Properties of the collection         Collection Type       Session         Resources       RemoteApp Programs         User Group       Value         REMOTEAPP PROGRAMS         Last refreshed on       Published RemoteApp programs [2 ffilter         Filter       Image: Collection RD Web Access         RemoteApp Program Name       Alias         Visible in RD Web Access       Iauncher         Iauncher       Iauncher	TASKS V TASKS V

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**".

<b>E</b>	Publish RemoteApp Prog	grams	_ 🗆 X
Select RemoteApp	programs		
RemoteApp Programs	Select the RemoteApp programs to publish RemoteApp program to the list, click Add.	to the QuickSession	Collection collection. To add a
Publishing	The RemoteApp programs are populated fr	rom	
	RemoteApp Program		Location ^
	About Java     Active Directory Administrative Ce     Active Directory Module for Wind     Administration Assistant for Wind     Administration Assistant for Wind     Adult Window Info (x64)     Autolt Window Info (x86)     Bginfo     Calculator     Character Map     Check For Updates     Check For Upd	%SYSTEMDRIVE%\ %SYSTEMDRIVE%\ %SYSTEMDRIVE%\ %SYSTEMDRIVE%\ %SYSTEMDRIVE%\ %SYSTEMDRIVE%\ %SYSTEMDRIVE%\ %SYSTEMDRIVE%\ %SYSTEMDRIVE%\ %SYSTEMDRIVE%\ III me RD Session Host s	Program Files/Java\jre1.8.0_2       Image: Constraint of the system 32\def data cases         Windows\system 32\def data cases       Windows\system 32\def data cases         Windows\system 32\def data cases       Windows\system 32\def data cases         App\Administrator\product\1       Program Files (x86)\Autolt3\         Program Files (x86)\Autolt3\       Windows\system 32\calc.exe         Windows\system 32\calc.exe       V         Program Files/Java\jre1.8.0_2       V         Program Files (vs86)\Autolt3\       >
	< Previo	ous Next >	Publish Cancel
<u> </u>	< Previo Open	ous Next >	Publish Cancel
E (a) ★ ↑ (b) ★ This PC (c)	< Previo Open Local Disk (C:) + space + space-launche	er v C	Publish Cancel
Crganize ▼ New folder	< Previo Open Local Disk (C:) > space > space-launche	ous Next> er ∨ Ĉ	Publish Cancel X Search space-launcher
Image: Constraint of the second s	< Previo Open  Local Disk (C:) > space > space-launche  Date modified	er v C	Publish     Cancel       Search space-launcher        ∰     ▼       ∭     ▼       Size
Image: Constraint of the second s	< Previo Open  Local Disk (C:)   space   space-launche  Date modified	er v C	Publish Cancel
Image: Second system     Image: Second system       Image: Second system     Im	< Previo Open  Local Disk (C:)  \$ space  \$ space-launche  Date modified	er v C Type Application	Publish Cancel
Image: Constraint of the second s	< Previo Open  Local Disk (C:) > space > space-launche  Date modified	er v C Type Application	Publish Cancel
Image: Second system     Image: Second system       Image: Second system     Im	< Previo Open  Local Disk (C:)  space  space-launche  Date modified	er v C	Publish     Cancel       Search space-launcher        B≡        Size       6 814 KB
<ul> <li>Crganize ▼ ↑ ↓ This PC</li> <li>Organize ▼ New folder</li> <li>Fax</li> <li>Crganize ↓ Name</li> <li>Crganize ↓ Name</li> <li>Crganize ↓ Name</li> <li>Crganize ↓ New folder</li> </ul>	< Previa Open Local Disk (C:) > space > space-launche Date modified	er v C Type Application	Publish Cancel
Image: Second system     Image: Second system       Organize     New folder       Organize     New folder       Image: Second system     Name       Image: Second system     Image: Second system       Image: Second	< Previa Open  Local Disk (C:)  space  space-launche  Date modified	er v C Type Application	Publish Cancel   Search space-launcher P   BEE Image: Concel   Size Image: Concel   6 814 KB 2
Example 1 Example 2 Organize ▼ New folder Fax Fax C C C C R Isuncher Isuncher Isuncher Name Isuncher Isuncher Name Isuncher	< Previa Open  Local Disk (C:)  space  space-launche  Date modified	er v C Type Application	Publish     Cancel       Search space-launcher        BEE<        Size        6 814 KB     2
<ul> <li>Corganize ▼ ↑ ↓ This PC</li> <li>Organize ▼ New folder</li> <li>Fay</li> <li>E</li> <li>C</li> <li>R</li> <li>I auncher</li> <li>R</li> <li>Name</li> <li>R</li> <li>Name</li> <li>R</li> <li>Name</li> <li>R</li> <li>Name</li> <li>R</li> <li>Name</li> <li>Name</li></ul>	< Previa Open Local Disk (C:) > space > space-launche Date modified	er v C Type Application	Publish Cancel
Image: Second system       Image: Second system         Image: Secon	< Previa Den Local Disk (C:) > space > space-launche Date modified	er v C	Publish Cancel
Image: Second state stat	< Previa Open  Local Disk (C:)  space  space-launche  Date modified	er v C Type Application	Publish     Cancel       Search space-launcher        BIII     III       Size     6 814 KB       2
<ul> <li>Corganize ▼ New folder</li> <li>Pave</li> <li>Corganize ▼ New folder</li> <li>Name</li> <li>Corganize ▼ New folder</li> <li>Name</li> <li>Corganize ▼ New folder</li> <li>Name</li> <li>Corganize ↑ New folder</li> <li>Name</li> <li></li></ul>	< Previa Definition Open  Local Disk (C:)  Space  Space-launche  Date modified	er v C	Publish Cancel
Image: Second state st	< Previa Open  Local Disk (C:)  space  space-launche  Date modified	er v C Type Application	Publish Cancel   Search space-launcher P   BEE< Image: Comparison of the state of the s

Рис. 25. Добавление нового приложения

После публикации нового RemoteApp перейдите в его контекстное меню и выберите "Edit Properties".

launcher	Edit Draparties	
	Eait 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**".

<b>a</b>	Properties
Launcher (QuickSee Show All General + Parameters - User Assignment + File Type Associati +	Properties       ■       ■       ×         essionCollection Collection)         Command-line Parameters       1       0 bo not allow any command-line parameters         Image: Allow any command-line parameters       Image: Allow any command-line parameters       2         Image: Allow any use the following command-line parameters       2
	OK Cancel Apply 3

Рис. 27. Выбор режима для приложения

#### 5.7.3. Рекомендации для 3CA 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 C3C.

#### 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 запуска приложений консоль mmc и открыть добавление инструментов.

🔚 Co	nsole1 - [Console Root]		
👼 File	Action View Favorites Window	Help	
4	New	Ctrl+N	
	Open	Ctrl+0	
	Save	Ctrl+S	
	Save As		There are no items to show in this view.
	Add/Remove Snap-in	Ctrl+M	
	Options		
	1 C:\Windows\system32\Isdiag.msc		
	Exit		
			1

Рис. 37. Добавление инструментов

			beletteu shaphins.	
nap-in Device Manager Disk Management Vertex Viewer Folder Group Policy Management Group Policy Management Editor Group Policy Object Editor Group Policy Starter GPO Editor Internet Information Services (. JP Security Monitor P Security Policy Management	Vendor Microsc Microsc Microsc Microsc Microsc Microsc Microsc Microsc Microsc Microsc	Add >	Console Root	Edit Extensions Remove Move Up Move Down
Link to Web Address	Microse v			Advanced

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»). Select Group Policy Object

#### 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: Local Computer Browse
	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 Finish Cancel
1 2 2	
elcome to the Group Policy W	/izard
elcome to the Group Policy W	lizard
elcome to the Group Policy W Browse for a Group Policy Obj Computers Users	lizard ject ? X
elcome to the Group Policy W Browse for a Group Policy Obj Computers Users Local Users and Groups compa	fizard
elcome to the Group Policy W Browse for a Group Policy Obj Computers Users Local Users and Groups compa Name Administrator ADMIN_ITHELP21RU DefaultAccount WDAGUtilityAccount Administrators Non-Administrators	rizard ject ? × atible with Local Group Policy: Group Policy Object Exists No No No No No No No Yes

 $\times$ 

Рис. 39. Выбор списка пользователей

OK

Cancel

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.

File Action View Favorites Window Help	
• 🔿 📶 🗟 🔟 📆 🔻	
Console Root	Sydem
Iccal Computer\Non-Administrators Policy	
🗸 🍕 User Configuration	Custom User Interface Setting State Comment
> 🧮 Software Settings	Edit policy retries
> 📔 Windows Settings	Eait <u>pointy setting</u>
Administrative Templates	Requirements:
> 🧮 Control Panel	At least Windows 2000
> 🚞 Desktop	See Custom User Interface - X
> 📫 Network	Description:
Shared Folders	Specifies an aitemate use 🔂 Custom User Interface Previous Setting Next Setting
Start Menu and Taskbar	The Evolution of the Ev
> 🎬 System	Vexplorer.exe) creates the One Conference Comment:
Windows Components	Windows interface, but O'Not comigured
🔁 All Settings	this setting to specify ar <ul> <li>Enabled</li> </ul>
	interface. If you enable the second
	me system stars the inter Disabled
	Supported on: At least Windows 2000
	To use this setting, copy
	interface program to a n
	or to your system drive. Options: Help:
	this setting, and type the
	interrace program, inclus
	teame extension, in the armiterace tile name (for example, explorer.exe)
	is not located in a folder SnippingTool.exe The Explorer program (%windir%\explorer.exe) creates the
	the Path environment va
	your system, enter the fu specify an alternate interface. If you enable this setting, the
	path to the file. System starts the interface you specify instead of Explorer.exe.
	If you disable this setting
	configure the setting in the setting in the setting in the setting and type
	and the system displays t the name of the interface program, including the file name
	interface. extension, in the Shell name text box. If the interface program file
	is not located in a folder specified in the Path environment
	Tip: To find the folders in Variable for your system, enter the fully qualified path to the file.
	the van environment va
	System Properties in Coli
	Environment Variables b
	then, in the System varia Tip: To find the folders indicated by the Path environment
	click Path. variable, click System Properties in Control Panel, click the
	Advanced tab, click the Environment Variables button, and then, in the Statement with the wild be added to the statement of t
	in the System variables box, click Path.
	OK Cancel Apply
	Evtended / Standard /

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 C3C.

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"

-	- Downloads	temApps	9/15/2018 10:19 AM	File folder	
Advanced Sec	urity Settings for explorer.exe		— 🗆	× der der	🐂 explorer.exe Properties
Name: Owner: Permissions	C:\Windows\explorer.exe Administrators (IUMP666\Administrators) 🔮 Char Auditing Effective Access	ge		der der der der der	General Digital Signatures Security Details Previous Versions Object name: C:\Windows\explorer.exe Group or user names: Impact APPUICATION PACKAGES
For additional in Permission entr	nformation, double-click a permission entry. To modi ries:	y a permission entry, select the e	ntry and click Edit (if available)	der der der der	ALL RESTRICTED APPLICATION PACKAGES     SYSTEM     Administrators (UMP666\Administrators)     Mathematications
Type F State Allow T Allow A Allow A Table Allow A Table Allow A	Principal IrustedInstaller Administrators (JUMP666\Administrators) SYSTEM ALL APPLICATION PACKAGES ALL RESTRICTED APPLICATION PACKAGES	Access Full control Read & execute Read & execute Read & execute Read & execute	Inherited from None None None None None	der der ation e cumen ation ation	To change permissions, click Edit. Edit Permissions for ALL APPLICATION PACKAGES Allow Deny Full control Modfy Read & execute Read Write Social cermissions
< Add Enable inher	Remove Edit ritance			> ation >cument >cument = ation >cument	For special permissions or advanced settings, click Advanced Advanced
		0	Cancel App	oly ation	320 KR

На скрине ниже пример настройки.

Рис. 42. Альтернативный жесткий вариант ограничения доступа

#### 5.8 Настройка групповых политик 3CA Windows

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

<b>H</b>	Group Policy Management
File Action View Window Help	
Group Policy Management     A Forest: SPACE.LOCAL     A A Domains     P A SPACE.LOCAL	Forest: SPACE.LOCAL Contents Name Domains
Group Policy Modeling	Group Policy Modeling

Puc. 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:

<u>R</u>				Gr	oup Policy Manage	ment
🔜 File Action View Wind	ow Help					
Group Policy Management		SPACE	LOCAL	-		
▲ A Forest: SPACE.LOCAL 1		Status	Linked Grou	up Policy Objects	Group Policy Inheritance	Deleg
Domains     SPACE.LOCAL     SPACE.LOCAL     Settificates	2 Create a GPO in this domain,	, and Link it her	e	status of Active	e Directory and SYSVOL re	plication
CSC-Auto	Link an Existing GPO Block Inheritance			1		

Puc. 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"**:

1	New GPO	x
Name: Connections Settings		
Source Starter GPO: (none)		~
	2 OK Can	icel

Puc. 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...":

<u>s</u>	Group Policy Managemen
File Action View Window Help	
Group Policy Management  Group Policy Management  Domains  Group Policy Management  Group Policy	Connections Settings           Scope         Details         Settings         Delegation           Links         Display links in this location:         SPACE.LOCAL
CSC-Auto Edit  Control Edit  Edit  Edit  Control Edit  Enforced Link Enabled Save Report	ACE.LOCAL No

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

4. В левом дереве выберите следующий раздел настроек:

"Computer Configuration\Policies\AdministrativeTemplates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections":

<b>1</b>	Group Po	licy Management Editor
<u>F</u> ile <u>A</u> ction <u>V</u> iew <u>H</u> elp		
🗢 🔿 🙍 🔂 🖬 🛐 🝸		
Connections Settings [DC01-12R2.SPACE.LOCAL] Policy	Connections	
⊿ ▲ Computer Configuration	Select an item to view its description.	Setting
A Policies		Automatic reconnection
1 D Software Settings		Allow users to connect remotely by using Remote Desktop S
2 A Administrative Templates: Policy definitions (A)		Deny logoff of an administrator logged in to the console ses
Control Panel		Configure keep-alive connection interval
Network		Limit number of connections
📔 Printers 🗮		Suspend user sign-in to complete app registration
Server		Set rules for remote control of Remote Desktop Services use
Start Menu and Taskbar		Select network detection on the server
System		E Select RDP transport protocols
3 A Windows Components		E Restrict Remote Desktop Services users to a single Remote D
	[	E Allow remote start of unlisted programs
	Group Po	licy Management Editor
<u>File</u> <u>Action</u> <u>View</u> <u>H</u> elp		
	7	
Maintenance Scheduler	Connections	
Network Assess Protection	Select an item to view its description.	Setting
Network Projector		E Automatic reconnection
OneDrive		Allow users to connect remotely by using Remote Desktop S
Online Assistance		Deny logoff of an administrator logged in to the console ses
Password Synchronization		Configure keep-alive connection interval
Portable Operating System		E Limit number of connections
Presentation Settings		Suspend user sign-in to complete app registration
4 🛛 🧰 Remote Desktop Services		Set rules for remote control of Remote Desktop Services use
KD Licensing		E Select PDP transport protocols
Kemote Desktop Connection Client		E Restrict Remote Deckton Services users to a single Remote D
Application Compatibility		Allow remote start of unlisted programs
6 Connections		Turn off Fair Share CPU Scheduling
Device and Resource Redirection	L	

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:

		Group Policy Management Editor				
Connections		Setting			State	Comment
limit number of connections		Automatic reconnection			Not configu	red No
dit policy setting	~	Allow users to connect remotely by using Remote Desktop S	Service	s	Not configu	red No
		Deny logoff of an administrator logged in to the console ses	sion		Not configu	red No
equirements: Not least Windows Server 2003		Configure keep-alive connection interval	2		Not configu	red No
teleast willdows berver 2005	1	E Limit number of connections			r figu	red No
escription:		E Suspend user sign-in to complete app registration	E	dit	rfigu	red No
pecifies whether Remote Desktop		E Set rules for remote control of Remote Desktop Services us	1	-ilter On	nfigu	red No
imultaneous connections to the		E Select network detection on the server	F	ilter Options	nfigu	red No
erver.		E Select RDP transport protocols	F	Re-Apply Filter	nfigu	red No
(		🗄 Restrict Remote Desktop Services users to a single Remote I	1	All Tasks	nfigu	red No
he number of Remote Desktop		E Allow remote start of unlisted programs	É		nfigu	red No
Services sessions that can be		E Turn off Fair Share CPU Scheduling	ŀ	Help	nfigu	red No
ctive on a server. If this number is xceeded, addtional users who try connect receive an error.						

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

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

<b>9</b>	Limit number of connections	_		x
Limit number of connections	Previous Setting Next Setting	]		
<ul> <li>○ Not <u>C</u>onfigured Comment:</li> <li>● <u>E</u>nabled 1</li> <li>○ <u>D</u>isabled Supported on</li> </ul>				<
Options:	At least Windows Server 2003 Help:			~
2				
RD Maximum Connections allowed 999999 Type 999999 for unlimited connection	Specifies whether Remote Desktop Services limits t simultaneous connections to the server. You can use this setting to restrict the number of R Desktop Services sessions that can be active on a se number is exceeded, additional users who try to con an error message telling them that the server is bus again later. Restricting the number of sessions imp performance because fewer sessions are demandin resources. By default, RD Session Host servers allow number of Remote Desktop Services sessions, and Desktop for Administration allows two Remote Des sessions.	emote erver. If nect re y and to roves g syster an unl Remote sktop Se	this ceive o try m limited ervices	=
	I o use this setting, enter the number of connection specify as the maximum for the server. To specify a number of connections, type 999999. If the status is set to Enabled, the maximum numbe connections is limited to the specified number con the version of Windows and the mode of Remote D	n unlin er of sistent Desktop	vant to nited with	,
	3 OK Cancel		<u>A</u> pply	

Puc. 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":

	Group Policy Management	t Editor		-
<u> </u>		· · ·		
Connections Restrict Remote Desktop Services users to a single Remote Desktop Services session	Setting           Setting           Image: Automatic reconnection           Image: Allow users to connect rem           Image: Allow users to connect rem	otely by using Remote Desktop Services	State Not configured Not configured	Comment No No
Edit <u>policy setting</u> Requirements:	E Configure keep-alive conne	rator logged in to the console session ection interval ns	Not configured Not configured Enabled	No No No
At least Windows Server 2003 Description: This policy setting allows you to restrict users to a single Remote Desktop Services session.	Suspend user sign-in to cor Set rules for remote control Select network detection or Select RDP transport protoco Restrict Remote Desktop Se Allow remote start of unlist Turn off Fair Share CPU Sch	nplete app registration of Remote Desktop Services user sessions n the server cols rvices users to a single Remote Desktop Services session ed programs reduling	Not configured Not configured Not configured Not configured Not configured Not configured	No No No No No No
Restrict Remote Designation	ktop Services users to	a single Remote Desktop Services se	ession – 🗖	
Restrict Remote Desktop	Services users to a single F	Remote Desktop Services session		
○ Not <u>C</u> onfigured Comm	ient:			^
<ul> <li><u>Enabled</u></li> <li><u>Disabled</u></li> </ul>				~
Suppo	At least Windov	vs Server 2003		^ ~
Options:		Help:		
		This policy setting allows you to restrict user Desktop Services session. If you enable this policy setting, users who le using Remote Desktop Services will be restri session (either active or disconnected) on th leaves the session in a disconnected state, th reconnects to that session at the next logon. If you disable this policy setting, users are al unlimited simultaneous remote connections Desktop Services. If you do not configure this policy setting, t not specified at the Group Policy level.	rs to a single Re og on remotely cted to a single hat server. If the ne user automat bowed to make s by using Remo his policy settin	mote by user ically ote g is
		зОКС	Cancel	Apply

Puc. 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

#### <u>JS 1</u> JS 2 JS N Launcher Launcher Launcher Агенты Агенты Агенты паролей паролей паролей LM 1 LM 2 LM N <...> Watcher Watcher Watcher Local Local Local storage storage storage TCP: 4222 TCP: 4222 TCP: 4222 TCP: 4222 TCP: 4222 Mono 1 Mono 2 Mono N TCP: 4244-NATS 1 TCP: 424 NATS 2 NATS N TCP: 4222 TCP: 4222 TCP: 4222 TCP: 4222 TCP: 4222 TCP: 4222 Storage 1 Storage 2 Storage N <...> Core 1 Core 2 Core N TCP: 5432 TCP: 5432 TCP: 5432 БД

#### 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)

- 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 Runtine Environment (x64)	
JCE	Java Cryptography Extension	
PostgreSQL DB	База данных PostgreSQL	<u>страница</u> <u>загрузки</u>
Tomcat	Контейнер сервлетов (х64)	<u>страница</u> <u>загрузки</u>
NATS	Платформа, реализующая систему обмена сообщениями (СОС)	<u>страница</u> <u>загрузки</u>
AutoIt	Скрипт для автоматизации выполнения задач в OC Microsoft Windows.	<u>страница</u> <u>загрузки</u>
Docker CE	Система контейнеров для Linux.	<u>страница</u> <u>загрузки</u>

# Приложение 1: Чек-лист подготовки инфраструктуры

- о Программное обеспечение на Сервер sPACE Mono (Base):
  - о Одна из ОС: CentOS 7-8, Ubuntu 22.04 и 24.04, Astra Linux «Орёл», Red OS «Муром» 7.3.2, ALT Linux 10;
  - о Файловая система ОС не находится в режиме **Read-only**;
  - о Установлен OpenSSL 1.1.1 и выше;
  - о Запущен Docker 24.0 и выше;
  - о Установлен Wget (GNU Wget);
  - о Установлен tar (tape archive);
  - о Установлен awk;
  - о Установлен sed (Stream EDitor).

#### о Программное обеспечение на Сервер 3CA Windows:

- o Microsoft Windows Server 2012-2019;
- о 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);
- о Установлен Windows PowerShell 5.1 и выше.
- о Программное обеспечение на Сервер 3CA Linux (SSH):
  - о Одна из ОС: CentOS 7-8, Ubuntu 22.04 и 24.04, Astra Linux «Орёл», Red OS «Муром» 7.3.2, ALT Linux 10;
  - о Установлен OpenSSL 1.1.1 и выше;
  - о Запущен Docker 24.0 и выше;
  - о Установлен Expect;
  - о Установлен Wget (GNU Wget);
  - о Установлен unzip;
  - о Установлен SSH (Secure Shell).

#### о Программное обеспечение на Сервер 3CA Linux (RDP):

- o OC ALT Linux 10;
- о Установлен OpenSSL 1.1.1 и выше;
- о Запущен Docker 24.0 и выше;
- о Установлен Expect;
- о Установлен Wget (GNU Wget);
- о Установлен unzip;
- о Установлен SSH (Secure Shell).
- о Выполнены все условия пункта 3.5 «**Требования к инфраструктуре**» из инструкции по развертыванию;
- о Обеспечена сетевая доступность открыты порты из таблицы 7 «Список требуемых к открытию сетевых портов» из инструкции по развертыванию.