perimetrix

SAFESPACE SERVER

РУКОВОДСТВО ПО АДМИНИСТРИРОВАНИЮ СЕРВЕРА

ПРАВОВАЯ ИНФОРМАЦИЯ

Все права защищены. Ни одна часть этого документа не может быть изменена, воспроизведена, сохранена в информационно-поисковой системе или передана в какой-либо форме или какими-либо средствами, включая электронными, механическими, методом фотокопирования, записи или иными способами без предварительного письменного разрешения ООО Периметрикс (Perimetrix).

По любым вопросам, касающимся использования этого документа, ознакомьтесь с общими положениями и условиями, доступными в компании Perimetrix. Названия Perimetrix, SafeSpace, SafeResource, SafeStore, SafePrint, DataSure и Cryptex, а также связанные с ними графические обозначения, являются собственностью ООО Периметрикс и не могут быть использованы без явного письменного разрешения компании Perimetrix. Любые другие упомянутые торговые знаки являются собственностью соответствующих владельцев и могут быть использованы только с разрешения этих владельцев. Руководства / инструкции пользователя, в том числе руководства по установке, инструкции по использованию и другие виды документов, предоставляются преимущественно в электронном формате. Для получения копии на бумажном носителе для этого документа или любого другого руководства по эксплуатации программного продукта обращайтесь в компанию Perimetrix.

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

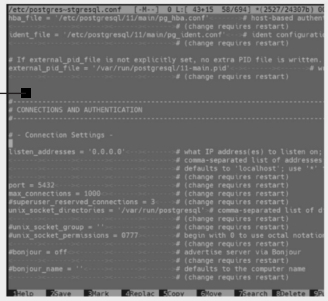
Perimetrix SafeSpace предоставляет надежные средства для управления конфиденциальными данными различного характера (коммерческая тайна, персональные данные и др). Как решение SafeSpace представляет собой совокупность приложений, устанавливаемых на сервер. На данном сервере работают базовые компоненты системы. При необходимости можно расширить функциональные возможности уже установленной системы за счет добавления дополнительных модулей.

В данном руководстве описываются вопросы, связанные с администрированием системы. Их рассмотрение позволит поддерживать производительность системы на соответствующем уровне, при необходимости выполнить ее аварийное восстановление, а также обеспечить непрерывность ит услуг.

В качестве справочного материала приводятся примеры для настройки параметров как в системе Linux, так и в консоли управления SafeSpace. Несмотря на все прилагаемые усилия повысить точность настраиваемых параметров, их значения, которые отображаются в соответствующих полях, могут отличаться и не совпадать с теми значениями, которые необходимо вводить при внедрении системы на базе существующей информационно–технической инфраструктуры заказчика.

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ, ИСПОЛЬЗУЕМЫЕ В ЭТОМ РУКОВОДСТВЕ

Снимок с экрана с процессом инсталляции.



Next, at the command prompt type **apt install postgresql–11** and press **Enter**. When prompted with `Do you want to continue? [y/n]`, type **y** and press **Enter**.

Входные данные или значения, запрашиваемые у пользователя.

Имена файлов, директорий или названия команд, требуемых для ввода пользователем.

Пункты меню, названия кнопок или пользовательские команды ввода.

If the message is displayed `Install these packages without verification? [y/n]`, type **y** and press **Enter**.

In the section **`IPv4 local connections`**, change the IP address from `127.0.0.1/32` to `0.0.0.0/0`.

Comment out the line in the **`IPv6 local connections`** section starting with host by adding a hash mark **`(#)`** at the beginning of the line.

Comment out the two lines in the section **`Allow replication connections from localhost`** to read:

Ссылки на текст или переменные в процессе инсталляции или настройки.

Образцы кода, включая переменные и ключевые слова, отображаемые системой.

```
# host    replication all        127.0.0.1/32          md5
# host    replication all        ::1/128               md5
```

At the command prompt type **su–postgres** and then press **Enter** to switch to PostgreSQL. The command prompt will change to show **`postgres@<server name>:~$`** (*see example below*).

Команды, ключевые слова и выражения.

```
postgres@debian:~$
```

To start PostgreSQL server, at the command prompt type **`psql`** and press **Enter**.

The command prompt will change to **`postgres=#`**

At the **`postgres=#`** prompt type:[21]

Сноски с дополнительной информацией. *Особое внимание* следует обратить на информацию, помеченную знаком ⚠

create database <*dbname1*>; and press **Enter**.
create user <*dbuser1*> with password '<*dbuser1pw*>'; and press **Enter**.
grant all privileges on database <*dbname1*> to <*dbuser1*>; and press **Enter**.
create database <*dbname2*>; and press **Enter**.
create user <*dbuser2*> with password '<*dbuser2pw*>'; and press **Enter**.
grant all privileges on database <*dbname2*> to <*dbuser2*>; and press **Enter**.

Имена файлов, директорий или названия команд, требуемых для ввода пользователем в *особом порядке.*

2 ЦЕЛЕВАЯ АУДИТОРИЯ ДОКУМЕНТА

Данное руководство предназначено для системных администраторов, *обладающих хорошим уровнем профессиональных компетенций и опытом работы по установке, настройке и эксплуатации систем из семейства Linux, а также дополнительных специальных приложений и решений.*

3 КРАТКО О РУКОВОДСТВЕ

В документе содержатся инструкции по внедрению SafeSpace 2.8 на базе серверов Debian GNU/Linux 9. В каждом конкретном случае настройка сервера будет зависеть от установленного дистрибутива и версии Linux, а также от доступных утилит.

Данное руководство разделено на тематические разделы для удобства поиска информации, необходимой пользователю.

В руководстве не содержатся сведения, касающиеся администрирования Linux, Tomcat или PostgreSQL, так как это не относится напрямую к SafeSpace. *См. соответствующую документацию,* предоставляемую компаниями–разработчиками для поиска информации, которая не описывается в данном руководстве.

Сведения, *выходящие за рамки* данного руководства:

a) PostgreSQL (установка, администрирование и эксплуатация базы данных, не связанная с SafeSpace);

b) Linux (установка, администрирование и эксплуатация, не связанная с SafeSpace);

c) Обновление и модернизация SafeSpace (описывается в отдельном документе, содержащем сведения об обновлениях или усовершенствованиях системы);

d) Мониторинг SafeSpace (описывается в отдельном документе);

e) Работа с отчетами в SafeSpace (описывается в отдельном документе);

f) Аварийное восстановление SafeSpace и действия по обеспечению непрерывности ит сервисов (описывается в отдельном документе).

4 РЕЗЕРВНОЕ КОПИРОВАНИЕ SAFESPACE

Существует несколько способов, доступных для резервного копирования и восстановления сервера SafeSpace. В данном руководстве особое внимание уделяется инструментам, отвечающим требованиям SafeSpace.

4.1. ОСТАНОВКА СЛУЖБ SAFESPACE

Перед резервным копированием сервера SafeSpace необходимо выполнить определенные действия, которые позволят улучшить качество резервных копий и повысят вероятность успеха любого потенциального восстановления.

Если все модули SafeSpace (например, SafeResource, SafePrint и др.) установлены на одном сервере, выполните следующее:

Войдите в консоль Linux на сервере SafeSpace под учетной записью root или как пользователь с правами администратора.

Остановите службы SafeSpace. Для этого в командной строке введите:

`/srv/safespace/bin/safespace stop all` и нажмите клавишу **Enter.**[1]

1. Если SafeResource установлен на отдельном сервере, сначала необходимо выполнить эту команду на сервере SafeResource, затем на сервере SafeSpace.

Если SafeResource установлен на отдельном сервере, необходимо выполнить следующее:

Во–первых, войдите в консоль Linux на сервере SafeResource под учетной записью root или как пользователь с правами администратора. В командной строке введите:

`/srv/safespace/bin/safespace stop` и нажмите клавишу **Enter**.

Во–вторых, войдите в консоль Linux на сервере SafeSpace под учетной записью root или как пользователь с правами администратора. В командной строке введите:

`/srv/safespace/bin/safespace stop all` и нажмите клавишу **Enter**.

Следующие два шага необходимо выполнить только на сервере SafeSpace:

Войдите в консоль Linux на сервере SafeSpace под учетной записью root или как пользователь с правами администратора.

1. Остановите службу Tomcat. Для этого в командной строке введите: **`service tomcat9 stop`** и нажмите клавишу **Enter**.

2. Перезапустите службу Postgresql. Для этого в командной строке введите: **`service postgresql restart`** и нажмите клавишу **Enter**.

Предполагается, что Postgresql расположен на том же сервере, что и SafeSpace. Обратите внимание, если базы данных Postgresql установлены на отдельном сервере, приведенные выше команды необходимо выполнять на этом сервере.

После остановки служб SafeSpace и Tomcat, а также перезагрузки Postgresql, можно приступать к резервному копированию сервера SafeSpace.

4.2. РЕЗЕРВНОЕ КОПИРОВАНИЕ SAFESPACE И SAFERESOURCE

4.2.1. Использование программного обеспечения для резервного копирования

Создать резервную копию сервера SafeSpace целиком можно с помощью любого инструмента, используемого компанией для резервного копирования (клонирование серверов, резервное копирование на ленту и т.д.). Однако инструкции по применению этих инструментов не рассматриваются в рамках данного документа. Для более подробной информации обратитесь к руководству пользователя соответствующего программного обеспечения, находящегося в распоряжении компании.

4.2.2. Использование инструментов SafeSpace

Описываемая процедура позволяет создать резервные копии для баз данных сервера SafeSpace и каталога `safespace`, расположенного на сервере. Обратите внимание, что резервные копии необходимо сделать для двух баз данных, имена которых задаются при подготовке сервера Linux для установки SafeSpace. Кроме того, базы данных могут быть установлены на отдельном сервере в зависимости от политик и требований компании, от информационно–коммуникационной инфраструктуры и т.д.

Этап 1: Войдите в систему Linux на сервере SafeSpace, для которого будет выполняться резервное копирование, под учетной записью root или как пользователь с правами администратора.

Шаг 1 Через консоль Linux создайте каталог, в котором будут храниться резервные копии. В рамках данного руководства создается каталог под названием **backup** в директории `/opt/` на сервере.

Например, введите в командной строке **`mkdir /opt/backup`** и нажмите клавишу **Enter**.[2]

Шаг 2 Создайте резервные копии для двух баз данных SafeSpace.

Для резервного копирования каждой базы данных выполните следующее:

В командной строке введите:

`/srv/safespace/bin/backupdb` ***`/<путь>/<имя файла создаваемой резервной копии> <IP–адрес сервера базы данных> <имя база данных> <имя пользователя БД> <пароль для пользователя БД>`*** и нажмите клавишу **Enter**.

Например, для резервного копирования первой базы данных в командной строке введите:

`/srv/safespace/bin/backupdb /opt/backup/file01 192.168.122.23 psql1 jksmith password123`

и нажмите клавишу **Enter**.

Повторно введите данную команду для второй базы данных, используя соответствующее имя базы данных и остальные учетные данные.

Для резервного копирования *второй* базы данных в командной строке введите: **`/srv/safespace/bin/backupdb /opt/backup/file02 192.168.122.23 psql2 jksmith password123`**

2. При необходимости можно использовать другое имя каталога и месторасположение в соответствии с политиками и требованиями компании.

и нажмите клавишу **Enter**.[3]

В зависимости от производительности сервера и размера базы данных может потребоваться некоторое время для выполнения резервного копирования. После его завершения появится сообщение под строкой с введенной командой. Чтобы убедиться, что резервное копирование было выполнено успешно, проверьте наличие резервной копии в каталоге назначения.

Например, в командной строке введите: **`ls -ls /opt/`** и нажмите клавишу **Enter**.

На экране отобразится список файлов с указанием размера, прав доступа и т.д.

Замените `/opt/backup` на тот путь, по которому были сохранены резервные копии баз данных.

3. ⚠ Имя базы данных, пользователь базы данных и пароль совпадают с теми значениями, которые указывались при установке СУБД (например, PostgreSQL) на сервер.

Этап 2: На данном этапе создается резервная копия каталога `safespace` на сервере. Например, достаточно будет создать архив для этого каталога (например, `.tar`). Существует много доступных способов в зависимости от политик и требований компании, а также имеющихся инструментов и др.

В рамках данного руководства каталог `safespace` будет заархивирован в файл под именем `ssbackup01012021.tar` в каталоге `/opt/backup/`.

С помощью консоли Linux перейдите в каталог `/opt/backup/`.

В командной строке введите:

`cd /opt/` и нажмите клавишу **Enter**.

Для создания архива можно использовать следующую команду:

`tar -C /srv/ -czvf <имя файла>.tar safespace` и нажмите клавишу Enter.

Например, в командной строке введите:

`tar -C /srv/ -czvf ssbackup01012021.tar safespace` и нажмите клавишу **Enter**.

В результате выполнения данной команды будет создан архив `ssbackup01012021.tar` в том каталоге, в котором вводилась команда.

Для более подробного описания, как использовать `tar` или другие инструменты для резервного копирования каталога `safespace`, см. соответствующую документацию для установленной системы Linux.[4]

4. ⚠ В целях обеспечения непрерывности ит сервисов и аварийного восстановления никогда не храните резервные копии на сервере, для которого они сделаны. Рекомендуется хранить резервные копии в другом надежном месте.

4.2.3. Using a hybrid method

Данный метод включает действия, выполняемые как в консоли Linux, так и в консоли управления SafeSpace. С помощью консоли управления SafeSpace экспортируется конфигурация сервера. С помощью консоли Linux экспортируется из базы данных определенная таблица, которая содержит закрытые ключи сертификатов, необходимые для создания и использования криптекс.

С помощью этих двух объектов сервер SafeSpace может быть восстановлен в пустую базу данных. В этом случае компания может сохранить

лог–файлы на неопределенный промежуток времени согласно политикам компании и требованиям законодательства без дополнительных затрат на поддержание большой базы данных.

На первом шаге выполняется экспорт текущей конфигурации сервера SafeSpace. *См. раздел, описывающий экспорт и импорт конфигураций, для более подробной информации и соответствующих инструкций*.

На втором шаге выполняется экспорт из базы данных таблицы documentkeys. Это необходимо в том случае, если компания использует криптекс (зашифрованные архивы). С помощью этих таблиц можно получить доступ к файлам криптекс, которые были созданы ранее.

В рамках данного руководства рассматривается экспорт необходимых таблиц из базы данных Postgresql. Для получения информации при работе с другими базами данных обратитесь в Perimetrix.

Обратите внимание, базы данных могут размещаться на другом сервере, отдельно от SafeSpace. Описываемые ниже действия должны выполняться на том сервере, на котором установлены базы данных (и Postgresql).

Войдите в систему Linux на сервере, на котором размещены базы данных, под учетной записью root или как пользователь с правами администратора.

Для перехода к Postgresql в командной строке введите:

`su - postgres` и нажмите клавишу **Enter**.

Для получения доступа к Postgresql введите **`psql`** и нажмите клавишу **Enter**.

Чтобы подключиться к базе данных, введите: **`\connect <имя базы данных>;`** и нажмите клавишу **Enter**.

Например, в командной строке введите:**`\connect psql1;`** и нажмите клавишу **Enter**.

После подключения к базе данных введите ниже команду для экспорта таблицы documentkeys:

`\copy documentkeys TO ‘documentkeys.csv’ CSV;` и нажмите клавишу Enter.

Для выхода из Postgresql введите **`\q`** и нажмите клавишу **Enter**.

Экспортированная таблица будет сохранена в виде файла по следующему пути:

```
/var/lib/postgresql/documentkeys.csv
```

Таблица documentkeys расположена в первой базе данных, которая задана в файле connection.properties, расположенном на сервере в каталоге /srv/safespace/conf/.[5]

4.3. РЕЗЕРВНОЕ КОПИРОВАНИЕ SAFERESOURCE

Резервное копирование SafeResource представляет собой относительно простой процесс, включающий создание резервных копий для двух основных объектов: каталогов в директории safespace и таблиц маршрутизации.[6]

5. ⚠ В целях обеспечения непрерывности ит сервисов и аварийного восстановления экспортированный файл конфигурации и файл documentkeys должны храниться в безопасном месте.

6. ⚠ В целях обеспечения непрерывности ит сервисов и аварийного восстановления резервные копии должны храниться в безопасном месте.

4.3.1. Предварительный этап резервного копирования сервера SafeResource

Приводимые инструкции применяются к серверу SafeResource, который установлен как отдельный сервер (т.е., не на одном сервере с SafeSpace; установка SafeSpace и SafeResource на одном сервере не рекомендуется).

Перед выполнением резервного копирования сервера SafeResource необходимо выполнить определенные действия, которые позволят улучшить качество резервных копий и повысить вероятность успеха любого потенциального восстановления.

Войдите в консоль Linux на сервере SafeResource под учетной записью root или как пользователь с правами администратора.

Остановите службы SafeResource. Для этого в командной строке введите:

`/srv/safespace/bin/safespace stop` и нажмите клавишу **Enter**.

4.3.2. Использование программного обеспечения для резервного копирования

Создать резервную копию сервера SafeResource целиком можно с помощью любого инструмента, используемого компанией для резервного копирования (клонирование серверов, резервное копирование на ленту и т.д.). Однако инструкции по применению этих инструментов не рассматриваются в рамках данного документа. Для более подробной информации обратитесь к руководству пользователя соответствующего программного обеспечения, находящегося в распоряжении компании.

4.3.3. Использование других инструментов

Ниже описывается процедура для резервного копирования сервера SafeResource.

Необходимо создать резервные копии для трех каталогов, расположенных в директории `safespace` (`bin`, `lib` и `conf`). Остальные каталоги не требуются. SafeResource выполняет переадресацию и использует таблицы маршрутизации для контроля трафика. Если используются таблицы маршрутизации, необходимо также создать резервную копию для файла, содержащего пути маршрутизации.

Для резервного копирования файлов и каталогов существуют различные методы.

Шаг 1

В рамках данного руководства каталоги `bin`, `lib` и `conf` будут заархивированы в файл под названием `srbackup01012021.tar` в каталог /opt/backup/.

Войдите в систему Linux на сервере SafeResource под учетной записью root или как пользователь с правами администратора.

Для перехода в каталог `/opt/backup/` в командной строке введите:

`cd /opt/` и нажмите клавишу **Enter**.

Для создания архива можно использовать следующую команду.

`tar -C /srv/safespace/ -czvf <имя файла>.tar bin conf lib` и нажмите клавишу **Enter**.

Например, в командной строке введите:

tar -C /srv/safespace/ -czvf srbackup01012021.tar bin conf lib и нажмите клавишу **Enter**.

В результате этого будет создан файл под названием `srbackup01012021.tar` в каталоге, из которого выполнялась команда. В архиве будут содержаться три каталога `bin`, `conf` и `lib`.

Шаг 2 Скопируйте таблицы маршрутизации (если используются) в другое место.

В целях обеспечения непрерывности ИТ сервисов и аварийного восстановления резервные копии должны храниться в безопасном месте.

4.4. ЗАПУСК СЛУЖБ SAFESPACE

После выполнения резервного копирования сервера SafeSpace необходимо перезапустить соответствующие службы. Так как SafeResource может быть установлен на отдельном сервере (*рекомендуется*), возможны два варианта последовательности действий для запуска необходимых служб.

Вариант 1: Все модули (включая SafeResource) установлены на одном сервере.

Войдите в консоль Linux на сервере SafeSpace под учетной записью root или как пользователь с правами администратора.

Для запуска службы Tomcat в командной строке введите:

service tomcat9 start и нажмите клавишу **Enter**.

Для запуска служб SafeSpace в командной строке введите:

/srv/safespace/bin/safespace start и нажмите клавишу **Enter**.

При использовании Zircon необходимо ввести команду, которая запускает все службы SafeSpace, включая Zircon.

Для этого в командной строке введите:

/srv/safespace/bin/safespace start all и нажмите клавишу **Enter**.

Вариант 2: SafeSpace и модуль SafeResource установлены на разных серверах.

Войдите в консоль Linux на сервере *SafeResource* под учетной записью root или как пользователь с правами администратора.

В командной строке введите:

/srv/safespace/bin/safespace start и нажмите клавишу **Enter**.

Войдите в консоль Linux на сервере *SafeSpace* под учетной записью root или как пользователь с правами администратора.

Для запуска службы Tomcat в командной строке введите:

service tomcat9 start и нажмите клавишу **Enter**.

Для запуска служб SafeSpace в командной строке введите:

`/srv/safespace/bin/safespace start` и нажмите клавишу **Enter**.

При использовании Zircon необходимо ввести команду, которая запускает все службы SafeSpace, включая Zircon.

Для этого в командной строке введите:

`/srv/safespace/bin/safespace start all` и нажмите клавишу **Enter**.

5 ВОССТАНОВЛЕНИЕ SAFESPACE

SafeSpace может быть восстановлен различными способами в зависимости от требований компании. При наличии резервных копий существует три метода восстановления системы. Процедуры восстановления для каждого из методов могут отличаться друг от друга в значительной степени, поэтому необходимо проявлять осторожность при их выполнении.

5.1. USING BACKUP SOFTWARE

Восстановить сервер SafeSpace можно с помощью любого инструмента, используемого компанией для резервного копирования и восстановления. Однако инструкции по применению этих инструментов не рассматриваются в рамках данного документа. Для более подробной информации обратитесь к руководству пользователя для соответствующего программного обеспечения.

5.2. USING SAFESPACE TOOLS

Выбор процедуры восстановления в значительной мере зависит от целей, которые компания преследует, восстанавливая SafeSpace. Кроме того, немаловажным фактором является, переустанавливаются ли базы данных на тот же сервер или новый, также могут учитываться и другие аспекты.*Обратите внимание:* необходимо восстановить две базы данных.

5.2.1. Only restoring the SafeSpace databases

Предполагается, что исходные базы данных (например, Postgresql), созданные на сервере, существуют. Если они были удалены, см. соответствующий раздел далее.

Шаг 1 Войдите в систему Linux на сервере SafeSpace, на который будут восстанавливаться базы данных из резервных копий, под учетной записью root или как пользователь с правами администратора.

В командной строке введите /**srv/safespace/bin/restoredb** ***/<путь>/<имя резервной копии, созданной ранее> <IP–адрес сервера БД> <имя базы данных> <имя пользователя БД> <пароль пользователя БД>*** и нажмите клавишу **Enter**.

Например:

Для восстановления первой базы данных в командной строке введите:

```
/srv/safespace/bin/restoredb /opt/backup/file01
192.168.122.23 psql1 jksmith password123
```

и нажмите клавишу **Enter**.

Повторно введите использованную выше команду для второй базы данных, заменив имя базы данных и остальные учетные данные на соответствующие значения.

Для восстановления второй базы данных в командной строке введите:

```
/srv/safespace/bin/restoredb /opt/backup/file02
192.168.122.23 psql2 jksmith password123
```

и нажмите клавишу **Enter**.

Шаг 2 В зависимости от производительности сервера и размера

	базы данных процесс восстановления может занять некоторое время (примерно несколько минут). После завершения восстановления появится сообщение под строкой с командой.
Шаг 3	Перезагрузите сервер и перезапустите SafeSpace. Убедитесь, что восстановление прошло успешно и система работает в штатном режиме.

5.2.2. Восстановление каталога safespace и баз данных

При необходимости восстановить каталог `safespace` и базы данных SafeSpace выполните действия, описанные ниже.

Предполагается, что исходные базы данных (например, Postgresql), созданные на сервере, существуют. Если они были удалены или восстановление сервера будет выполняться с нуля (установлены/переустановлены базы данных Postgresql), см. соответствующий раздел далее.

Шаг 1	Восстановите каталог `safespace` и его содержимое. Для этого необходимо выполнить следующее: В рамках данного руководства каталог safespace был вложен в архив (`.tar`). Поэтому, предварительно необходимо извлечь его из архива в каталог `/srv/`. Войдите на сервер SafeSpace, который восстанавливается, под учетной записью root или как пользователь с правами администратора. Скопируйте файл `.tar`, который был создан для резервной копии сервера SafeSpace. Распакуйте архив в каталог.[7] Для извлечения данных их архива в командной строке введите: **`tar -xzvf <path to and name of tar file> -C <path to location>`** и нажмите клавишу **Enter**. Например, в командной строке введите: **`tar -xzvf ssbackup01012021.tar -C /srv/`** и нажмите клавишу **Enter**. С помощью данной команды архив с именем `ssbackup01012021.tar` будет распакован в каталог `/srv/`. Каталог safespace и его содержимое будут доступны по следующему пути `/srv/`. Для более подробной информации об использовании `tar` или других инструментов для создания резервных копий для каталога `safespace` см. соответствующую документацию для установленной системы Linux.
Шаг 2	Восстановите базы данных SafeSpace. Для этого выполните следующее: Если резервные копии баз данных хранятся в другом месте, скопируйте их на сервер SafeSpace.
Шаг 3	Войдите на сервере SafeSpace, для которого будут восстанавливаться базы данных, под учетной записью root или как

7. ⚠ Если только содержимое каталога `safespace` было заархивировано (например, `/bin`, `/certs`, `/conf`), предварительно создайте каталог `safespace` и распакуйте архив в него.

	пользователь с правами администратора.
Шаг 4	В командной строке введите **/srv/safespace/bin/restoredb /<путь>/<имя созданной ранее резервной копии> <IP-адрес сервера БД> <имя базы данных> <имя пользователя БД> <пароль для пользователя БД>** и нажмите клавишу **Enter**. Например: Для восстановления первой базы данных в командной строке введите: **/srv/safespace/bin/restoredb /opt/backup/file01 192.168.122.23 psql1 jksmith password123** и нажмите клавишу **Enter**. Повторно введите использованную выше команду для второй базы данных, заменив имя базы данных и остальные учетные данные на соответствующие значения. Для восстановления второй базы данных в командной строке введите: **/srv/safespace/bin/restoredb /opt/backup/file02 192.168.122.23 psql2 jksmith password123** и нажмите клавишу **Enter**. В зависимости от производительности сервера и размера базы данных процесс восстановления может занять некоторое время (примерно несколько минут). После завершения восстановления появится сообщение под строкой с командой.
Шаг 5	Перезагрузите сервер и перезапустите SafeSpace. Убедитесь, что восстановление прошло успешно и система работает в штатном режиме.

5.2.3. Восстановление в переустановленные или новые базы данных

Если базы данных (на сервере Postgresql) были переустановлены, а каталог safespace остался без изменений, необходимо выполнить следующие действия.

Шаг 1	Создайте базы данных. Базы данных могут размещаться на одном сервере с SafeSpace или на другом сервере, отдельно от SafeSpace, в зависимости от политик и требований компании, от информационно-технологической инфраструктуры и других факторов. Инструкции по созданию БД доступны в *Руководстве по подготовке сервера Linux*. Для восстановления потребуются имена баз данных, имена пользователей и пароли. Шаги с 2 по 6 выполняются на сервере SafeSpace.
Шаг 2	Восстановите базы данных SafeSpace. Для этого выполните следующее: Если резервные копии баз данных хранятся в другом месте, скопируйте их на сервер SafeSpace.

Войдите на сервере SafeSpace, на который будут восстанавливаться базы данных, под учетной записью root или как пользователь с правами администратора.

В командной строке введите:

/srv/safespace/bin/restoredb /*<имя созданной ранее резервной копии> <IP-адрес сервера БД> <имя базы данных> <имя пользователя БД> <пароль для пользователя БД>*
и нажмите клавишу **Enter**.

Например:

Для восстановления первой базы данных в командной строке введите:

/srv/safespace/bin/restoredb /opt/backup/file01 192.168.122.23 psql1 jksmith password123 и нажмите клавишу **Enter**.

Повторно введите использованную выше команду для второй базы данных, заменив имя базы данных и остальные учетные данные на соответствующие значения.

Для восстановления второй базы данных введите в командной строке:

/srv/safespace/bin/restoredb /opt/backup/file02 192.168.122.23 psql2 jksmith password123 и нажмите клавишу **Enter**.

В зависимости от производительности сервера и размера базы данных процесс восстановления может занять некоторое время (примерно несколько минут). После завершения восстановления появится сообщение под строкой с командой.

Шаг 3

Проверьте сведения о базах данных и учетных записях в двух файлах: `connection.properties` и `arc.connection.properties`, расположенных в каталоге `/srv/safespace/conf/`. Для этого выполните следующее:

В рамках данного руководства используется Midnight Commander (mc). Описываемые действия могут выполняться также с помощью других утилит в зависимости от политик и требований компании, установленных приложений и т.д.

Войдите на сервере SafeSpace под учетной записью root или как пользователь с правами администратора.

Отредактируйте файл `connection.properties`, расположенный в каталоге `/srv/safespace/conf/`. Для этого:

В командной строке введите **mc** и нажмите клавишу **Enter**.

Перейдите в каталог `/srv/safespace/conf/` и выберите файл `connection.properties`.

Нажмите **F4** для его редактирования.

В блоке `#postgreSQL settings` проверьте и при необходимо-

сти измените следующие переменные параметры:

hibernate.connection.url=jdbc:postgresql://*<IP-адрес сервера>/<имя первой базы данных>*

hibernate.connection.username=*<имя пользователя для первой базы данных>*

hibernate.connection.password=<пароль для указанного выше пользователя>

Нажмите **F2** для сохранения изменений, если они были внесены.

Нажмите клавишу **Enter** для подтверждения сохранения.

Нажмите **F10** для выхода из файла.

Оставаясь в Midnight Commander в каталоге /srv/safespace/conf/, выберите файл `arc.connection.properties`.

Нажмите **F4** для его редактирования.

В блоке `#postgreSQL settings` проверьте и при необходимости измените следующие переменные параметры.

hibernate.connection.url=jdbc:postgresql://*<IP-адрес сервера>/<имя второй базы данных>*

hibernate.connection.username=*<имя пользователя для второй базы данных>*

hibernate.connection.password=*<пароль для указанного выше пользователя>*

Нажмите **F2** для сохранения изменений, если они были внесены.

Нажмите клавишу **Enter** для подтверждения сохранения.

Нажмите **F10** для выхода из файла.

Шаг 4

Проверьте сведения о базах данных и учетных записях в двух файлах: `connection.properties` и `arc.connection.properties`, расположенных в каталоге `/var/lib/tomcat9/webapps/solar/WEB-INF/classes/`. Для этого выполните следующее:

Обратите внимание, что эти файлы совпадают с файлами, находящимися в каталоге `/srv/safespace/conf/`. После проверки сведений в файлах `connection.properties` и `arc.connection.properties` в каталоге `/srv/safespace/conf/` их можно скопировать в каталог `/var/lib/tomcat9/webapps/solar/WEB-INF/classes/`.[8]

Войдите на сервере SafeSpace под учетной записью root или как пользователь с правами администратора.

В командной строке введите **mc** и нажмите клавишу **Enter**.

Перейдите в каталог `/var/lib/tomcat9/webapps/solar/WEB-`

8. В рамках данного руководства используется Midnight Commander (mc). Описываемые действия могут выполняться также с помощью других утилит в зависимости от политик и требований компании, установленных приложений и т.д.

INF/classes/ и выберите файл connection.properties.

Нажмите **F4** для его редактирования.

В блоке #postgreSQL settings проверьте и при необходимости измените следующие переменные параметры:

hibernate.connection.url=jdbc:postgresql://*<IP-адрес сервера>/<имя первой базы данных>*

hibernate.connection.username=*<имя пользователя для первой базы данных>*

hibernate.connection.password=*<пароль для указанного выше пользователя>*

Нажмите **F2** для сохранения изменений, если они были внесены.

Нажмите клавишу **Enter** для подтверждения сохранения.

Нажмите **F10** для выхода из файла.

Оставаясь в Midnight Commander в каталоге /var/lib/tomcat9/webapps/solar/WEB-INF/classes/, выберите файл arc.connection.properties.

Нажмите **F4** для его редактирования.

В блоке #postgreSQL settings проверьте и при необходимости измените следующие переменные параметры:

hibernate.connection.url=jdbc:postgresql://*<IP-адрес сервера>/<имя второй базы данных>*

hibernate.connection.username=*<имя пользователя для второй базы данных>*

hibernate.connection.password=*<пароль для указанного выше пользователя>*

Нажмите **F2** для сохранения изменений, если они были внесены.

Нажмите клавишу **Enter** для подтверждения сохранения.

Нажмите **F10** для выхода из файла.

Шаг 5 Проверьте параметры Apache Tomcat. Для этого:

С помощью Midnight Commander перейдите в каталог /lib/systemd/system/.

Выберите файл tomcat9.service и нажмите **F4** для его редактирования.

В блоке, обозначенном # Configuration, проверьте наличие текста, приведенного ниже (*обратите внимание, что текст вводится без разрывов строк*). Если переменная окружения отсутствует, добавьте ее в файл.

Environment="CATALINA_OPTS=-Xms1024M -Xmx1024M -server -Dorg.apache.el.parser.SKIP_IDENTIFIER_CHECK=true"

Нажмите **F2** для сохранения изменений, если они были внесены.

Нажмите клавишу **Enter** для подтверждения сохранения.

Нажмите **F10** для выхода из файла.

Нажмите **F10** для выхода из Midnight Commander.

Перезагрузите сервер и перезапустите SafeSpace. Убедитесь, что восстановление прошло успешно и система работает в штатном режиме.

5.2.4. Полное восстановление на новый (пустой) сервер

Восстановите SafeSpace на пустой сервер, следуя инструкциям ниже.[9]

Шаг 1 Подготовьте сервер согласно инструкциям, содержащимся в руководстве по подготовке сервера Linux. Для восстановления потребуются имена баз данных, имена пользователей и пароли.

Шаг 2 Восстановите каталог `safespace` и его содержимое. Для этого выполните следующее:

В рамках данного руководства каталог `safespace` был вложен в архив (`.tar`). Поэтому, предварительно необходимо извлечь его из архива в каталог `/srv/`.

Войдите на сервер SafeSpace под учетной записью root или как пользователь с правами администратора.

Скопируйте файл `.tar`, который был создан для резервной копии сервера. Распакуйте архив в каталог `/srv/`.[10]

Для извлечения данных из архива в командной строке введите:

tar -xzvf *<path to and name of tar file>* -C *<path to location>* и нажмите клавишу **Enter**.

Например, в командной строке введите:

tar -xzvf ssbackup01012021.tar -C /srv/ и нажмите клавишу **Enter**.

С помощью данной команды архив с именем `ssbackup01012021.tar` будет распакован в каталог `/srv/`. Каталог `safespace` и его содержимое будут доступны по следующему пути `/srv/safespace/`.

Для более подробной информации об использовании tar или других инструментов для создания резервных копий для каталога `safespace` см. соответствующую документацию для установленной Linux.

Шаг 3 Восстановите базы данных SafeSpace. Для этого выполните следующее:

9. ⚠ При изменении MAC-адреса сервера необходимо получить *новую лицензию*. Свяжитесь с Perimetrix за дополнительной информацией.

10. ⚠ Если только содержимое каталога `safespace` было заархивировано (например, `/bin`, `/certs`, `/conf`), предварительно создайте каталог `safespace` и распакуйте в него архив.

Если резервные копии баз данных хранятся в другом месте, скопируйте их на сервер SafeSpace. Войдите на сервер SafeSpace, на который будут восстанавливаться базы данных, под учетной записью root или как пользователь с правами администратора.

At the command prompt type **/srv/safespace/bin/restoredb /<путь>/<имя созданной ранее резервной копии> <IP-адрес сервера БД> <имя базы данных> <имя пользователя БД> <пароль для пользователя БД>** и нажмите клавишу **Enter**.

Например:

Для восстановления первой базы данных в командной строке введите:

/srv/safespace/bin/restoredb /opt/backup/file01 192.168.122.23 psql1 jksmith password123 и нажмите клавишу **Enter**.

Повторно введите использованную выше команду для второй базы данных, заменив имя базы данных и остальные учетные данные на соответствующие значения.

Для восстановления второй базы данных в командной строке введите:

/srv/safespace/bin/restoredb /opt/backup/file02 192.168.122.23 psql2 jksmith password123 и нажмите клавишу **Enter**.

В зависимости от производительности сервера и размера базы данных процесс восстановления может занять некоторое время (примерно несколько минут). После завершения восстановления появится сообщение под строкой с командой.

Шаг 4

Проверьте сведения о базах данных и учетных записях в двух файлах: `connection.properties` и `arc.connection.properties`, расположенных в каталоге /srv/safespace/conf/. Для этого выполните следующее:

В рамках данного руководства используется Midnight Commander (mc). Описываемые действия могут выполняться также с помощью других утилит в зависимости от политик и требований компании, установленных приложений и т.д.

Войдите на сервер SafeSpace под учетной записью root или как пользователь с правами администратора.

Отредактируйте файл `connection.properties`, расположенный в каталоге `/srv/safespace/conf/`. Для этого:

В командной строке введите **mc** и нажмите клавишу **Enter**.

Перейдите в каталог `/srv/safespace/conf/` и выберите файл `connection.properties`.

Нажмите **F4** для его редактирования.

В блоке `#postgreSQL settings` проверьте и при необходимо-

сти измените следующие переменные параметры:

hibernate.connection.url=jdbc:postgresql://*<IP-адрес сервера>/<имя первой базы данных>*

hibernate.connection.username=*<имя пользователя для первой базы данных>*

hibernate.connection.password=<пароль для указанного выше пользователя>

Нажмите **F2** для сохранения изменений, если они были внесены.

Нажмите клавишу **Enter** для подтверждения сохранения.

Нажмите **F10** для выхода из файла.

Оставаясь в Midnight Commander в каталоге `/srv/safespace/conf/`, выберите файл `arc.connection.properties`.

Нажмите **F4** для его редактирования.

В блоке `#postgreSQL settings` проверьте и при необходимости измените следующие переменные параметры:

hibernate.connection.url=jdbc:postgresql://*<IP-адрес сервера>/<имя второй базы данных>*

hibernate.connection.username=*<имя пользователя для второй базы данных>*

hibernate.connection.password=*<пароль для указанного выше пользователя>*

Нажмите **F2** для сохранения изменений, если они были внесены.

Нажмите клавишу **Enter** для подтверждения сохранения.

Нажмите **F10** для выхода из файла.

Шаг 5

Проверьте сведения о базах данных и учетных записях в двух файлах: `connection.properties` и `arc.connection.properties`, расположенных в каталоге `/var/lib/tomcat9/webapps/solar/WEB-INF/classes/`. Для этого выполните действия, описанные ниже.

Обратите внимание, что эти файлы совпадают с файлами, находящимися в каталоге `/srv/safespace/conf/`. После проверки сведений в файлах `connection.properties` и `arc.connection.properties` в каталоге `/srv/safespace/conf/` их можно скопировать в каталог `/var/lib/tomcat9/webapps/solar/WEB-INF/classes/`.[11]

Войдите на сервер SafeSpace под учетной записью root или как пользователь с правами администратора.

В командной строке введите **mc** и нажмите клавишу **Enter**.

Перейдите в каталог `/var/lib/tomcat9/webapps/solar/WEB-`

11. В рамках данного руководства используется Midnight Commander (mc). Описываемые действия могут выполняться также с помощью других утилит в зависимости от политик и требований компании, установленных приложений и т.д.

INF/classes/ и выберите файл connection.properties.

Нажмите **F4** для его редактирования.

В блоке #postgreSQL settings проверьте и при необходимости измените следующие переменные параметры:.

hibernate.connection.url=jdbc:postgresql://*<IP-адрес сервера>/<имя первой базы данных>*

hibernate.connection.username=*<имя пользователя для первой базы данных>*

hibernate.connection.password=<пароль для указанного выше пользователя>

Нажмите **F2** для сохранения изменений, если они были внесены.

Нажмите клавишу **Enter** для подтверждения сохранения.

Нажмите **F10** для выхода из файла.

Оставаясь в Midnight Commander в каталоге /var/lib/tomcat9/webapps/solar/WEB-INF/classes/, выберите файл arc.connection.properties.

Нажмите **F4** для его редактирования.

В блоке #postgreSQL settings проверьте и при необходимости измените следующие переменные параметры:

hibernate.connection.url=jdbc:postgresql://*<IP-адрес сервера>/<имя второй базы данных>*

hibernate.connection.username=*<имя пользователя для второй базы данных>*

hibernate.connection.password=*<пароль для указанного выше пользователя>*

Нажмите **F2** для сохранения изменений, если они были внесены.

Нажмите клавишу **Enter** для подтверждения сохранения.

Нажмите **F10** для выхода из файла.

Шаг 6 Проверьте параметры Apache Tomcat. Для этого:

С помощью Midnight Commander перейдите в каталог /lib/systemd/system/.

Выберите файл tomcat9.service и нажмите **F4** для его редактирования.

В блоке, обозначенном # Configuration, проверьте наличие текста, приведенного ниже (*обратите внимание, что текст вводится без разрывов строк*). Если переменная окружения отсутствует, добавьте ее в файл.

	Environment="CATALINA_OPTS=-Xms1024M -Xmx1024M -server -Dorg.apache.el.parser.SKIP_IDENTIFIER_CHECK=true" Нажмите **F2** для сохранения изменений, если они были внесены. Нажмите клавишу **Enter** для подтверждения сохранения. Нажмите **F10** для выхода из файла. Нажмите **F10** для выхода из Midnight Commander.
Шаг 7	Перезагрузите сервер и перезапустите SafeSpace. Убедитесь, что восстановление прошло успешно и система работает в штатном режиме.

5.2.5. Использование гибридного метода

При использовании гибридного метода необходимо учитывать определенные факторы. Например, базы данных SafeSpace не восстанавливаются с помощью данного метода.

Гибридный метод используется преимущественно для «очистки» баз данных, т.е. удаляется всё их содержимое. Чтобы данные не были утеряны, необходимо сделать резервную копию баз данных и сохранить ее в безопасном месте.

Описываемый метод может быть использован при необходимости соблюсти условия политик компании и требования законодательства. Например, если данные нужно хранить в течение пяти лет, данный метод позволит выполнить это требование и при этом сохранить оптимальную производительность сервера SafeSpace.

Гибридный метод состоит из определенных шагов, которые должны быть выполнены в указанном порядке:

1. Экспортировать текущую конфигурацию сервера SafeSpace (см. алгоритм выполнения далее в этом руководстве).
2. Остановить службы SafeSpace (при необходимости и SafeResource).
3. Остановить службу Tomcat.
4. Перезапустить службу Postgresql
5. Экспортировать из базы данных таблицу documentkeys (см. выше описание резервного копирования с помощью гибридного метода в данном руководстве).
6. Удалить базы данных.
7. Создать базы данных.
8. Проверить параметры подключения.
9. Применить лицензии SafeSpace.
10. Импортировать файл documentkeys.
11. Запустить службу Tomcat.
12. Импортировать файл конфигурации SafeSpace.
13. Создать и применить конфигурацию.
14. Запустить службы SafeSpace (при необходимости и SafeResource)

Шаг 1	Экспортируйте текущую конфигурацию сервера SafeSpace (см. алгоритм выполнения далее в данном руководстве). Шаги 2 и 3 выполняются на сервере SafeSpace.
Шаг 2	Если все модули SafeSpace (например, SafeResource, SafePrint и др.) установлены на одном сервере, выполните следующие действия: Войдите в консоль Linux на сервере SafeSpace под учетной записью root или как пользователь с правами администратора.

	Остановите службы SafeSpace. Для этого в командной строке введите: **`/srv/safespace/bin/safespace stop all`** и нажмите клавишу **Enter**. Если SafeResource установлен на отдельном сервере, необходимо выполнить следующее: Во–первых, войдите в консоль Linux на сервере *SafeResource* под учетной записью root или как пользователь с правами администратора. В командной строке введите: **`/srv/safespace/bin/safespace stop`** и нажмите клавишу Enter. Во–вторых, войдите в консоль Linux на сервере *SafeSpace* под учетной записью root или как пользователь с правами администратора. В командной строке введите: **`/srv/safespace/bin/safespace stop all`** и нажмите клавишу **Enter**.
Шаг 3	Данный шаг необходимо выполнить *только* на сервере SafeSpace. Войдите в консоль Linux на сервере SafeSpace под учетной записью root или как пользователь с правами администратора. Остановите службу Tomcat. Для этого в командной строке введите: **`service tomcat9 stop`** и нажмите клавишу **Enter**. Шаги с 4 по 7 выполняются на сервере Postgresql. *Обратите внимание*, что Postgresql может размещаться как на одном сервере с SafeSpace, так и на отдельном сервере. Во втором случае (если Postgresql установлен на отдельном сервере) войдите в консоль Linux на этом сервере.
Шаг 4	Перезапустите Postgresql. Для этого в командной строке введите: **`service postgresql restart`** и нажмите клавишу **Enter**.
Шаг 5	Экспортируйте таблицу `documentkeys` из базы данных (*см. выше описание резервного копирования с помощью гибридного метода в данном руководстве*).
Шаг 6	Удалите две базы данных Postgresql с сервера. Для этого: Войдите в консоль Linux на сервере, на котором установлен Postgresql, под учетной записью root или как пользователь с правами администратора. Для перехода к Postgresql в командной строке введите:

su - postgres и нажмите клавишу **Enter**.

Для получения доступа к Postgresql введите **psql** и нажмите клавишу **Enter**.

Для удаления первой базы данных, в строке postgres=# введите:

drop database *<dbname1>;* и нажмите клавишу **Enter**.

Где ***dbname1*** – это имя первой базы данных, используемой SafeSpace.

Для удаления второй базы данных в строке postgres=# введите:

drop database *<dbname2>;* и нажмите клавишу **Enter**.

Где ***dbname2*** – это имя второй базы данных, используемой SafeSpace.

Обратите внимание, данные действия не влияют на пользователей и пароли, существующие до этого.

Шаг 7

Создайте две базы данных Postgresql на сервере. Для этого выполните следующие действия:

Войдите в консоль Linux на сервере, на котором установлен Postgresql, под учетной записью root или как пользователь с правами администратора.

Для перехода к Postgresql в командной строке введите:

su - postgres и нажмите клавишу **Enter**.

Для получения доступа к Postgresql введите **psql** и нажмите клавишу **Enter**.

Для создания первой базы данных, в строке postgres=# введите:

create database *<dbname1>;* и нажмите клавишу **Enter**.

Где ***dbname1*** – это имя первой базы данных, используемой SafeSpace. *Рекомендуется оставить прежнее имя базы данных*. См. далее, если вводится другое имя бд.

Если требуется добавить нового пользователя базы данных (согласно политикам или требованиям компании), создайте нового пользователя. Для этого в командной строке введите:

create user *<dbuser1>* with password '*<dbuser1pw>*'; и нажмите клавишу **Enter**.

Необходимо предоставить все привилегии для пользователя базы данных (для уже существующего или созданного заново). Для этого в командной строке введите:

grant all privileges on database *<dbname1>* to *<dbuser1>;* и нажмите клавишу **Enter**.

Вторая база данных SafeSpace создается аналогичным способом. Для этого:

В командной строке введите:

create database *<dbname2>;* и нажмите клавишу **Enter**.

Где ***dbname2*** – это имя второй базы данных, используемой SafeSpace. *Рекомендуется оставить имя базы данных, которое использовалось ранее.* См. далее, если вводится другое имя бд.

Если требуется добавить нового пользователя базы данных (согласно политикам или требованиям компании), создайте нового пользователя. Для этого в командной строке введите:

create user *<dbuser2>* with password '*<dbuser2pw>*';
и нажмите клавишу **Enter**.

Где ***dbuser2*** – это имя пользователя второй базы данных, а ***dbuser2pw*** – это пароль для него. *Рекомендуется использовать прежнее имя пользователя и пароль для него.* См. далее, если вводится другое имя пользователя и/или пароль.

Необходимо предоставить все привилегии для пользователя базы данных (для уже существующего или созданного заново). Для этого в командной строке введите:

grant all privileges on database *<dbname2>* to *<dbuser2>*;
и нажмите клавишу **Enter**.

После этого в командной строке введите:

\q и нажмите клавишу **Enter**.

Введите **exit** и нажмите клавишу **Enter**, чтобы вернуться в командную строку Linux.

Шаги 8 и 9 выполняются на сервере SafeSpace.

Шаг 8–A

Проверьте сведения о базах данных и учетных записях в двух файла: `connection.properties` и `arc.connection.properties`, расположенных в каталоге `/srv/safespace/conf/`. Для этого выполните следующие действия:

В рамках данного руководства используется Midnight Commander (mc). Описываемые действия могут выполняться также с помощью других утилит в зависимости от политик и требований компании, установленных приложений и т.д.

Войдите на сервере SafeSpace под учетной записью root или как пользователь с правами администратора.

Отредактируйте файл `connection.properties`, расположенный в каталоге `/srv/safespace/conf/`. Для этого:

В командной строке введите **mc** и нажмите клавишу **Enter**.

Перейдите в каталог `/srv/safespace/conf/` и выберите файл `connection.properties`.

Нажмите **F4** для его редактирования.

В блоке #postgreSQL settings проверьте и при необходимости измените следующие переменные параметры:

hibernate.connection.url=jdbc:postgresql://*<IP-адрес сервера>/<имя первой базы данных>*

hibernate.connection.username=*<имя пользователя для первой базы данных>*

hibernate.connection.password=*<пароль для указанного выше пользователя>*

Нажмите **F2** для сохранения изменений, если они были внесены.

Нажмите клавишу **Enter** для подтверждения сохранения.

Нажмите **F10** для выхода из файла.

Оставаясь в Midnight Commander в каталоге /srv/safespace/conf/, выберите файл arc.connection.properties.

Нажмите **F4** для его редактирования.

В блоке #postgreSQL settings проверьте и при необходимости измените следующие переменные параметры:

hibernate.connection.url=jdbc:postgresql://*<IP-адрес сервера>/<имя второй базы данных>*

hibernate.connection.username=*<имя пользователя для второй базы данных>*

hibernate.connection.password=*<пароль для указанного выше пользователя>*

Нажмите **F2** для сохранения изменений, если они были внесены.

Нажмите клавишу **Enter** для подтверждения сохранения.

Нажмите **F10** для выхода из файла.

Шаг 8–Б

Проверьте сведения о базах данных и учетных записях в двух файлах: connection.properties и arc.connection.properties, расположенных в каталоге /var/lib/tomcat9/webapps/solar/WEB-INF/classes/. Для этого выполните действия, описанные ниже.

Обратите внимание, что эти файлы совпадают с файлами, находящимися в каталоге /srv/safespace/conf/. После проверки сведений в файлах connection.properties и arc.connection.properties в каталоге /srv/safespace/conf/ их можно скопировать в каталог /var/lib/tomcat9/webapps/solar/WEB-INF/classes/.

В рамках данного руководства используется Midnight Commander (mc). Описываемые действия могут выполняться также с помощью других утилит в зависимости от политик

и требований компании, установленных приложений и т.д.

Войдите на сервер SafeSpace под учетной записью root или как пользователь с правами администратора.

В командной строке введите **mc** и нажмите клавишу **Enter**.

Перейдите в каталог /var/lib/tomcat9/webapps/solar/WEB-INF/classes/ и выберите файл connection.properties.

Нажмите **F4** для его редактирования.

В блоке #postgreSQL settings проверьте и при необходимости измените следующие переменные параметры:

hibernate.connection.url=jdbc:postgresql://*<IP-адрес сервера>/<имя первой базы данных>*

hibernate.connection.username=*<имя пользователя для первой базы данных>*

hibernate.connection.password=*<пароль для указанного выше пользователя>*

Нажмите **F2** для сохранения изменений, если они были внесены.

Нажмите клавишу **Enter** для подтверждения сохранения.

Нажмите **F10** для выхода из файла.

Оставаясь в Midnight Commander в каталоге /var/lib/tomcat9/webapps/solar/WEB-INF/classes/, выберите файл arc.connection.properties.

Нажмите **F4** для его редактирования.

В блоке #postgreSQL settings проверьте и при необходимости измените следующие переменные параметры:

hibernate.connection.url=jdbc:postgresql://*<IP-адрес сервера>/<имя второй базы данных>*

hibernate.connection.username=*<имя пользователя для второй базы данных>*

hibernate.connection.password=*<пароль для указанного выше пользователя>*

Нажмите **F2** для сохранения изменений, если они были внесены.

Нажмите клавишу **Enter** для подтверждения сохранения.

Нажмите **F10** для выхода из файла.

Нажмите F10 для выхода из Midnight Commander.

Шаг 9 Примените лицензию SafeSpace. Для этого выполните следующие действия:

Войдите на сервере SafeSpace под учетной записью root или как пользователь с правами администратора.

Для обновления лицензии в командной строке введите:

/srv/safespace/bin/update_license и нажмите клавишу Enter.

В командной строке появится запрос на файл лицензии, предоставляемый Perimetrix. Имя файла лицензии заканчивается на `.lic` и обычно расположен в каталоге `/certs/`. Обратите внимание, что файл лицензии может храниться и в другом месте в зависимости от использованного способа установки сервера. В рамках данного руководства файл лицензии (`abc_company.lic`) и открытый ключ сертификата (`cs-id.pem`) находятся в каталоге `/certs/`.

В строке `License file:` введите:

/**srv/safespace/certs/abc_company.lic** и нажмите клавишу **Enter**. (Замените имя файла на соответствующее имя лицензии, которая предоставляется Perimetrix).

В строке `Public key:` введите:

/srv/safespace/certs/cs-id.pem и нажмите клавишу **Enter**.

Если действия были выполнены корректно, то через несколько секунд появится сообщение Update license successful.

Шаг 10 выполняется на сервере, на котором размещается Postgresql

Шаг 10

Импортируйте файл `documentkeys`. Для этого выполните следующие действия:

Войдите в консоль Linux на сервере, на котором установлен Postgresql, под учетной записью root или как пользователь с правами администратора.

Для перехода к Postgresql в командной строке введите:

su - postgres и нажмите клавишу **Enter**.

Для получения доступа к Postgresql введите **psql** и нажмите клавишу **Enter**.

Затем в командной строке введите: **\connect *<dbname1>;***
и нажмите клавишу **Enter** (где ***dbname1*** – это имя первой базы данных, созданной ранее).

Далее в командной строке введите: **\copy documentkeys FROM 'documentkeys.csv' DELIMITER ',' CSV;**

и нажмите клавишу **Enter**.

Для выхода из Postgresql введите: **\q** и нажмите клавишу Enter.

Введите **exit** и нажмите клавишу **Enter** для возврата в командную строку Linux.

	Шаг 11 выполняется на сервере SafeSpace.
Шаг 11	На сервере SafeSpace запустите службу Tomcat. Для этого выполните следующее: Войдите в консоль Linux на сервере SafeSpace под учетной записью root или как пользователь с правами администратора. Для запуска службы Tomcat в командной строке введите: **`service tomcat9 start`** и нажмите клавишу **Enter**. Шаги 12 и 13 выполняются с помощью консоли управления SafeSpace.
Шаг 12	Импортируйте файл конфигурации SafeSpace. См. алгоритм импорта в соответствующем разделе данного руководства.
Шаг 13	Создайте и примените новую конфигурацию. См. последовательность действий в соответствующем разделе данного руководства. Шаг 14 выполняется на сервере SafeSpace с помощью консоли Linux.
Шаг 14	Запустите службы SafeSpace. Для этого выполните следующие действия: Так как SafeResource может быть установлен на отдельном сервере (*рекомендуется*), возможны два варианта последовательности действий для запуска необходимых служб.
	Вариант 1: Все модули (включая SafeResource) установлены на одном сервере. Войдите в консоль Linux на сервере SafeSpace под учетной записью root или как пользователь с правами администратора. Для запуска службы Tomcat в командной строке введите: **`service tomcat9 start`** и нажмите клавишу **Enter**. Для запуска служб SafeSpace в командной строке введите: **`/srv/safespace/bin/safespace start`** и нажмите клавишу Enter. При использовании Zircon необходимо ввести команду, которая запускает все службы SafeSpace, включая Zircon. Для этого в командной строке введите: **`/srv/safespace/bin/safespace start all`** и нажмите клавишу **Enter**.

Вариант 2: SafeSpace и модуль SafeResource установлены на разных серверах.

Войдите в консоль Linux на сервере SafeResource под учетной записью root или как пользователь с правами администратора.

В командной строке введите:

`/srv/safespace/bin/safespace start` и нажмите клавишу Enter.

Войдите в консоль Linux на сервере SafeSpace под учетной записью root или как пользователь с правами администратора.

Для запуска службы Tomcat в командной строке введите:

`service tomcat9 start` и нажмите клавишу **Enter**.

Для запуска служб SafeSpace в командной строке введите:

`/srv/safespace/bin/safespace start` и нажмите клавишу Enter.

При использовании Zircon необходимо ввести команду, которая запускает все службы SafeSpace, включая Zircon.

Для этого в командной строке введите:

`/srv/safespace/bin/safespace start all` и нажмите клавишу **Enter**.

После этого убедитесь, что система работает в штатном режиме.

5.3. РОТАЦИЯ ЛОГ–ФАЙЛОВ

Функция `logrotate` позволяется упростить задачи по администрированию систем, которые генерируют большое количество лог–файлов. Также можно выполнить ротацию, сжатие, удаление лог–файлов и другие операции. Кроме того, функцию `logrotate` можно запускать ежедневно, еженедельно, ежемесячно и т.д. или при соблюдении определенных условий (например, размер лог–файла достиг определенного размера).

Данную функцию рекомендуется выполнять, так как при работе SafeSpace и SafeResource может создаваться большое количество лог–файлов (необходимых, например, для качественного аудита).

Лог–файлы для SafeSpace и SafeResource расположены в каталоге `/srv/safespace/log/`.

В рамках данного руководства используется Midnight Commander, при необходимости можно применить и другие инструменты.

Описываемые действия необходимо выполнить на каждом сервере SafeSpace и SafeResource.

Шаг 1 Создайте и отредактируйте файл под именем `safespace` в каталоге `/etc/logrotate.d/`. Для этого:

Войдите на сервер Linux под учетной записью root или как

пользователь с правами администратора.

Для создания (или редактирования) файла под именем safespace в командной строке введите:

mcedit /etc/logrыotate.d/safespace и нажмите клавишу **Enter**.

Шаг 2

Отредактируйте файл safespace, созданного на предыдущем шаге. Для этого необходимо выполнить следующее:

Для серверов SafeSpace без установленного Zircon, в файл добавьте представленный ниже текст между словами --- start copy --- и --- end copy ---.

--- start copy ---

```
/srv/safespace/log/safespace-nm.log {

weekly

rotate 10

size 300M

copytruncate

compress

delaycompress

}

/srv/safespace/log/safespace-nls.log {

monthly

rotate 10

size 50M

copytruncate

compress

delaycompress

}
```

--- end copy ---

Для серверов SafeSpace с установленным Zircon, в файл добавьте представленный ниже текст между словами --- start copy --- и --- end copy ---.

--- start copy ---

```
/srv/safespace/log/safespace-nm.log {

weekly
```

```
rotate 10

size 300M

copytruncate

compress

delaycompress

}

/srv/safespace/log/safespace-nls.log {

monthly

rotate 10

size 50M

copytruncate

compress

delaycompress

}

/srv/safespace/log/zircon.log {

monthly

rotate 10

size 50M

copytruncate

compress

delaycompress

}
```

--- end copy ---

Для серверов SafeResource (если SafeResource установлен на отдельном сервере), в файл добавьте представленный ниже текст между словами --- start copy --- и --- end copy ---.

--- start copy ---

```
/srv/safespace/log/safespace-nm.log {

weekly

rotate 10

size 300M

copytruncate
```

```
compress

delaycompress

}

--- end  copy ---
```

Нажмите **F2** для сохранения файла.

Нажмите клавишу **Enter** для подтверждения действия.

Нажмите **F10** для выхода из файла.

5.4. АВТОМАТИЧЕСКИЙ ЗАПУСК SAFESPACE / SAFERESOURCE

После перезагрузки сервера службы SafeSpace и SafeResource автоматически не запускаются. В данном разделе содержится инструкция для настройки автоматического запуска служб SafeSpace и/или SafeResource.

Описываемая функция требует службу `rc-local`. Если эта служба отсутствует на сервере, необходимо ее установить.

В рамках данного руководства используется Midnight Commander, при необходимости можно применить и другие инструменты.[12]

12. ⚠ Описываемые шаги должны быть выполнены в указанной последовательности.

На всех серверах SafeSpace и SafeResource выполните следующее:

Шаг 1 Создайте файл с именем `rc-local.service` в директории `/etc/systemd/system/`.

Войдите в консоль Linux под учетной записью root или как пользователь с правами администратора.

Для создания файла `rc-local.service` в командной строке введите:

`mcedit /etc/systemd/system/rc-local.service` и нажмите клавишу **Enter**.

Шаг 2 Отредактируйте файл `rc-local.service`, созданного на предыдущем шаге. Для этого в файл добавьте представленный ниже текст между словами `--- start  copy ---` и `--- end  copy ---`.

```
--- start  copy ---

[Unit]

Description=/etc/rc.local

ConditionPathExists=/etc/rc.local

[Service]

Type=forking

ExecStart=/etc/rc.local start

TimeoutSec=0
```

```
StandardOutput=tty

RemainAfterExit=yes

SysVStartPriority=99

[Install]

WantedBy=multi-user.target
```

--- end copy ---

Нажмите **F2** для сохранения файла.

Нажмите клавишу **Enter** для подтверждения сохранения.

Нажмите **F10** для выхода из файла.

Для серверов SafeSpace (с установленным или без установленного Zircon):

Шаг 1 Создайте файл под названием `rc.local` в директории `/etc/`.

Если файл `rc.local` уже существует, достаточно добавить соответствующую команду перед “`exit 0`”. Подробнее см. ниже Шаг 2.

Войдите в консоль Linux под учетной записью root или как пользователь с правами администратора.

Для создания (или редактирования) файла `rc.local` в командной строке введите:

`mcedit /etc/rc.local` и нажмите клавишу **Enter**.

Шаг 2 Отредактируйте файл `rc.local`.

Для этого в файл добавьте следующий текст между словами --- `start copy` --- и --- `end copy` --- .

--- `start copy` ---

```
#!/bin/sh -e

#

# rc.local

#

# This script is executed at the end of each multiuser
runlevel.

# Make sure that the script will "exit 0" on success or
any other

# value on error.

#

# In order to enable or disable this script just change
the execution
```

```
# bits.

#

# By default this script does nothing.

#

# If SafeResource is running on the same server as
SafeSpace,

# uncomment the following line changing the path and
filename as appropriate.

# iptables-restore /opt/tab

#

# The following line starts SafeSpace without Zircon
(default).

/srv/safespace/bin/safespace start

# If using Zircon, comment the above line and uncomment
the following line.

# /srv/safespace/bin/safespace start all

exit 0
```

--- end copy ---

Нажмите **F2** для сохранения изменений в файле.

Нажмите клавишу **Enter** для подтверждения действия.

Нажмите **F10** для выхода из файла.

Только для серверов SafeResource (установленных на отдельном сервере):

Шаг 1 Создайте файл под названием `rc.local` в директории `/etc/`.

Если файл `rc.local` уже существует, достаточно добавить соответствующую команду перед "`exit 0`". Подробнее см. ниже Шаг 2.

Войдите в консоль Linux под учетной записью root или как пользователь с правами администратора.

Для создания (или редактирования) файла `rc.local` в командной строке введите:

`mcedit /etc/rc.local` и нажмите клавишу **Enter**.

Шаг 2 Отредактируйте файл `rc.local`.

Для этого в файл добавьте следующий текст между словами --- start copy --- и --- end copy ---.

--- start copy ---

```
#!/bin/sh -e

#

# rc.local

#

# This script is executed at the end of each
multiuser runlevel.

# Make sure that the script will "exit 0" on success or
any other

# value on error.

#

# In order to enable or disable this script just change
the execution

# bits.

#

# By default this script does nothing.

#

# The following line applies the IP routing tables (if
saved in a file).

# Update the path and file name as required.

iptables-restore /opt/tab

# The following line starts SafeResource.

/srv/safespace/bin/safespace start

exit 0
```

--- end copy ---

Нажмите **F2** для сохранения изменений в файле.

Нажмите клавишу **Enter** для подтверждения действия.

Нажмите **F10** для выхода из файла.

For all SafeSpace and SafeResource servers do the following. Предоставьте привилегии на запуск для файла `rc.local`. Для этого в командной строке введите: **`chmod +x /etc/rc.local`** и нажмите клавишу **Enter**.

Активируйте автозапуск для службы. Для этого в командной строке введите: **`systemctl enable rc-local`** и нажмите клавишу **Enter**.

Запустите службу. Для этого в командной строке введите: **`systemctl start rc-local`** и нажмите клавишу **Enter**.

6 УСТАНОВКА ИЛИ ОБНОВЛЕНИЕ ЛИЦЕНЗИИ SAFESPACE

Переустановка и/или обновление лицензии SafeSpace может потребоваться в разных случаях (например, обновление сборки сервера, приобретение дополнительных модулей и т.д.).[13]

Для установки и/или обновления лицензии необходимо выполнить следующее:

Войдите на сервер SafeSpace под учетной записью root или как пользователь с правами администратора. Для обновления лицензии в командной строке введите:

`/srv/safespace/bin/update_license` и нажмите клавишу **Enter**.

В командной строке появится запрос на файл лицензии, предоставляемый Perimetrix. Имя файла лицензии заканчивается на .lic и он обычно расположен в каталоге `/certs/`. Обратите внимание, что файл лицензии может храниться и в другом месте в зависимости от использованного способа установки сервера. В рамках данного руководства файл лицензии (`abc_company.lic`) и открытый ключ сертификата (`cs-id.pem`) находятся в каталоге `/certs/`.

В строке `License file:` введите:

`/srv/safespace/certs/abc_company.lic` и нажмите клавишу **Enter**. (Замените имя файла на соответствующее имя лицензии, которая предоставляется Perimetrix).

В строке `Public key:` введите:

`/srv/safespace/certs/cs-id.pem` и нажмите клавишу **Enter**.

Если действия были выполнены корректно, то через несколько секунд появится сообщение Update license successful.

13. ⚠ Если для компании–клиента необходимо, чтобы компания Perimetrix использовала свой сертификат для создания файла лицензии, то клиент должен предоставить закрытый ключ сертификата и MAC–адрес сетевого интерфейса, который будет использовать SafeSpace. ⚠ Для установки и активации лицензии потребуется файл лицензии и открытый ключ, связанный с закрытым ключом, который был использован для создания лицензии. ⚠ Имя и расположение открытого ключа может отличаться в зависимости от политик и требований компании.

7 ЭКСПОРТ И ИМПОРТ КОНФИГУРАЦИЙ

Рекомендуется регулярно экспортировать текущую актуальную конфигурацию для сервера SafeSpace. Данную операцию необходимо также выполнять до момента внесения каких–либо изменений. Это позволит восстановить предыдущую конфигурацию в случае возникновения ошибки или выполнения непреднамеренных действий при работе с системой.[14]

14. Для экспорта текущих настроек конфигурации, необходимо сначала создать и применить новую конфигурацию.

7.1. ЭКСПОРТ КОНФИГУРАЦИИ

Для экспорта текущей конфигурации необходимо выполнить следующее:

Войдите в консоль управления SafeSpace.

В области меню выберите **Разное**, затем **Экспорт конфигурации**.

Оставьте поле **Код конфигурации** пустым и нажмите **Экспорт**.

Экспорт конфигурации.

Текущая конфигурация будет сохранена в виде файла `.xml` в папке для загрузок браузера на компьютере. Файлу будет присвоено имя `export.xml`. Если такой файл уже существует, то к именам скачиваемых файлов добавляется цифровой индекс, который увеличивается автоматически (например, `export (1).xml` и т.д.).

Обратите внимание, что предыдущие (архивированные) конфигурации можно экспортировать, набрав соответствующий код (например, `CONF#0025`) в поле Код конфигурации. Имя экспортированного файла также будет содержать код конфигурации (например, `export_CONF#0025.xml`).

7.2. ИМПОРТ КОНФИГУРАЦИИ

Для импорта ранее экспортированной конфигурации необходимо выполнить следующее:

Войдите в консоль управления SafeSpace.

Измените (при необходимости) последний использованный номер конфигурации. Для этого измените номер прямо в экспортированном файле `.xml` или с помощью правил нумерации (**Справочники / Правила нумерации**) на сервере. При импорте конфигурации будет использован следующий доступный номер.

В области меню выберите **Разное**, затем **Импорт конфигурации**.

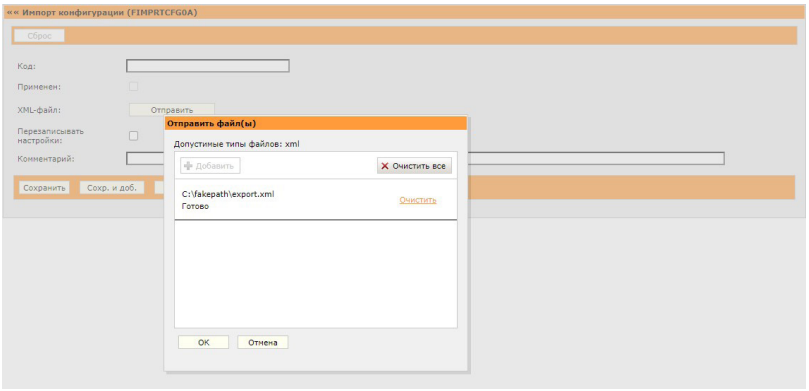
Нажмите **Создать**.

Затем нажмите **Отправить**.

В диалоговом окне **Отправить файл(ы)** нажмите **Добавить** и перейдите к ресурсу, на котором хранится файл конфигурации.

Выберите нужный файл конфигурации (например, `export.xml`) и нажмите **Открыть**.

Нажмите **ОК**.



Импорт конфигурации.

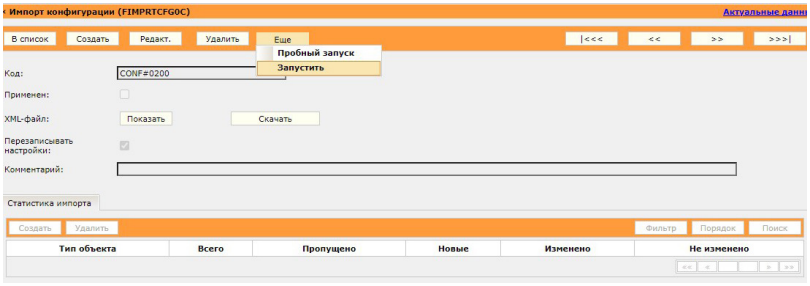
На форме **Импорт конфигурации** установите флажок **Перезаписывать настройки.**[15]

Добавьте необходимую информацию или комментарии в поле **Комментарий**.

Введите код в поле **Код** (например, `CONF#0025`). Как правило, он должен превышать значение кода последней конфигурации, примененной на сервере.

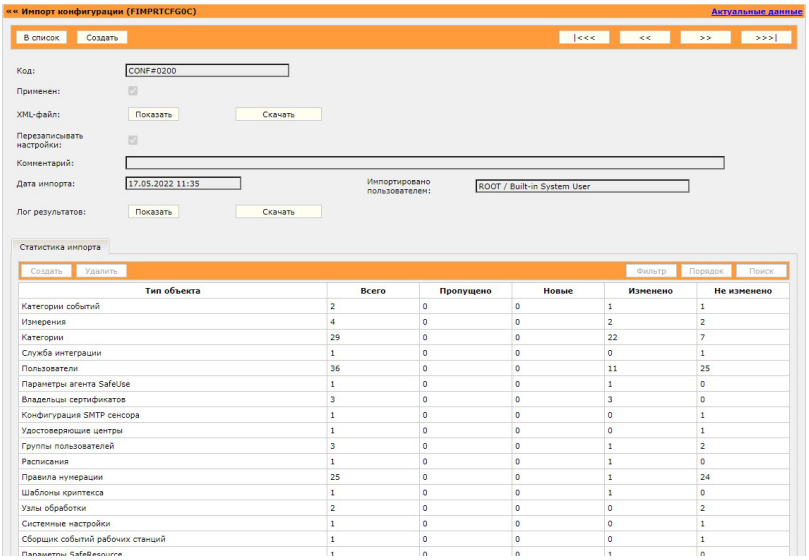
Нажмите **Сохранить**.

Нажмите **Еще**, затем выберите **Запустить** из раскрывающегося меню.



Применение импортированной конфигурации.

В нижней части экрана появится статистика импорта в виде таблицы с типами объектов и выполненными действиями: **пропущено, новые, изменено, не изменено**. Все возникшие ошибки будут отображены под таблицей и отмечены *красным цветом*.



Статистика импорта конфигурации.

15. ⚠ Новые измерения и категории будут добавлены, при этом существующие измерения и категории останутся без изменений. ⚠ Обратите внимание, что при импорте в пустую базу данных не имеет принципиального значения, установлен или не установлен флажок **Перезаписывать настройки**, так как отсутствуют данные для перезаписи. ⚠ Если флажок **Перезаписывать настройки** не установлен, тогда параметры с заданными значениями будут проигнорированы. Только вновь созданные объекты (например, контейнеры) будут добавлены в конфигурацию.

Если ошибки не были обнаружены, перейдите в меню **Справочники**, затем **Конфигурации**.

Нажмите **Создать новую конфигурацию**.

Нажмите **Сохранить**.

Затем нажмите **Применить конфигурацию**.

Снова выберите в области меню **Конфигурации** для просмотра списка конфигураций и убедитесь, что последняя из них имеет состояние **Примененная**.

8 УСТРАНЕНИЕ НЕПОЛАДОК

При возникновении проблем с SafeSpace необходимо проверить некоторые параметры. Если с помощью приведенных рекомендаций не удалось решить проблему, обратитесь в службу технической поддержки Perimetrix.

8.1. ПРОБЛЕМЫ С ЛИЦЕНЗИЕЙ

Проблема: сервер SafeSpace был запущен, а узел обработки и/или связанные службы не запускаются.

Возможная причина №1: срок лицензии SafeSpace истек.
Необходимо проверить: проверьте статус лицензии через консоль управления SafeSpace.

Войдите в консоль управления SafeSpace.

В области меню выберите **Технические настройки** / **Данные лицензии**.

Проверьте дату лицензии в поле **Дата конца лицензии**.

Если срок лицензии истек, обратитесь в Perimetrix для ее обновления.

Возможная причина №2: MAC–адрес сервера SafeSpace был изменен.
Необходимо проверить: сравните MAC–адрес, указанный в лицензии SafeSpace, с MAC–адресом сетевого интерфейса сервера.

Войдите в консоль управления SafeSpace.

В области меню выберите **Технические настройки** / **Данные лицензии**.

Проверьте MAC–адрес в поле MAC–адрес службы имен. MAC–адрес в консоли управления SafeSpace отображается без двоеточия (**:**).

Войдите на сервер Linux под учетной записью root или как пользователь с правами администратора.

В командной строке введите **ip a** и нажмите клавишу **Enter**.

Проверьте MAC–адрес, привязанный к сетевому интерфейсу, который используется сервером SafeSpace. В данном случае MAC–адрес состоит из шести двухсимвольных сегментов, разделенных двоеточием (**:**).

Сравните два MAC–адреса.

Если MAC–адреса не совпадают, обратитесь в Perimetrix за новой лицензией. Обратите внимание, для компании Perimetrix необходимо предоставить закрытый ключ сертификата, если компания–клиент планирует использовать свои сертификаты.

8.2. ПРОБЛЕМЫ С ПОДКЛЮЧЕНИЕМ К КОНСОЛИ УПРАВЛЕНИЯ SAFESPACE

Проблема: отсутствует подключение к консоли управления SafeSpace.

Возможная причина №1: указан неправильный URL–адрес в адресной строке браузера.
Необходимо проверить: проверьте корректность введенного URL–адреса.

URL–адрес должен соответствовать шаблону:
***<имя или IP-адрес>:<порт>*/solar**

Например: **192.168.120.225:8080/solar**

Возможная прична №2: возникла проблема со службой Apache Tomcat (например, она не запущена).
Solution: перезапустите службу `tomcat9` service.

Войдите на сервер Linux под учетной записью root или как пользователь с правами администратора.

Для запуска службы Tomcat в командной строке введите:

`service tomcat9 restart` и нажмите клавишу **Enter**.

Попробуйте снова войти в консоль управления. Если до сих пор отсутствует подключение к консоли управления, обратитесь в службу технической поддержки Perimetrix.

8.3. ПРОБЛЕМЫ ПРИ РАБОТЕ С КРИПТЕКСОМ

Проблема: невозможно создавать, открывать или редактировать файлы в криптексе.

Возможная причина: узел обработки или соответствующие службы не запущены.
Необходимо проверить: убедитесь, что службы SafeSpace запущены.

Войдите в консоль управления SafeSpace.

В области меню перейдите в **Мониторинг** / **Статус узлов обработки**.

Убедитесь, что в колонке **Состояние** отображается значение **Запущен**.

Нажмите в колонке **Код** на код в виде гиперссылки для соответствующего узла обработки.

На вкладке **Службы** в колонке **Состояние** для всех привязанных служб должен отображаться статус **Запущен** (особенно для **Службы хранения ключей** и **Службы шифрованного хранения**).

Если все службы запущены, проблема может быть связана с конфигурацией SafeSpace.

Если у некоторых или у всех служб отсутствует статус **Запущен**, то возможно истек срок действия сертификатов. Проверить срок действия можно в файле `safespace-nm.log`, который расположен в каталоге `/srv/safespace/log/` на сервере Linux.

Если проблема остается нерешенной, обратитесь в службу технической поддержки Perimetrix.

8.4. ПРОБЛЕМЫ С КОНФИГУРАЦИЯМИ

Проблема: рабочие станции не получили конфигурации или конфигурации не были применены в консоли управления SafeSpace.

Возможная причина: узел обработки или соответствующие службы

не запущены.
Необходимо проверить: убедитесь, что службы SafeSpace запущены.

	Войдите в консоль управления SafeSpace. В области меню перейдите в **Мониторинг** / **Статус узлов обработки**. Убедитесь, что в колонке Состояние отображается значение **Запущен**.
	Нажмите в колонке **Код** на код в виде гиперссылки для соответствующего узла обработки. На вкладке **Службы** в колонке **Состояние** для всех привязанных служб должен отображаться статус **Запущен**. Если некоторые или все службы не запущены, проверьте лог–файлы на наличие ошибок. Лог–файлы SafeSpace расположены в каталоге `/srv/safespace/log/` на сервере Linux.
	Если проблема остается нерешенной, обратитесь в службу технической поддержки Perimetrix. Обратите внимание, если только некоторые рабочие станции не получают конфигурации, причина ошибки может быть связана с этими компьютерами. Для более подробной информации см. *Раздел об устранении неполадок в руководстве по администрированию SafeUse*.

8.5. ПРОБЛЕМА С ПАРОЛЕМ ДЛЯ ПОЛЬЗОВАТЕЛЯ ROOT ПРИ ВХОДЕ В КОНСОЛЬ УПРАВЛЕНИЯ SAFESPACE

Если пароль для учетной записи root, которая используется для входа в консоль управления, *был утерян*, для восстановления его значения по умолчанию необходимо выполнить следующие действия:[16]

16. ⚠ Данная учетная запись используется только для входа в веб–консоль управления SafeSpace, а не в консоль Linux.

Войдите в консоль Linux на сервере, на котором установлен Postgresql, под учетной записью root или как пользователь с правами администратора.

Для перехода к Postgresql в командной строке введите:
`su - postgres` и нажмите клавишу **Enter**.

Для получения доступа к Postgresql в командной строке введите: **`psql`** и нажмите клавишу **Enter**.

Затем в командной строке введите: **`\connect <имя первой базы данных>;`** и нажмите клавишу **Enter**. Например, в командной строке введите: **`\connect psql1;`** и нажмите клавишу **Enter**.

Затем в командной строке введите:
`UPDATE system_user SET passw_hash = '99-87-16-22123-71-12880121107100-98-123722469' WHERE login = 'root';` и нажмите клавишу **Enter**.[17]

17. Данная команда вводится одной строкой, без разрывов строк.

Это позволяет сбросить пароль для учетной записи root до значения по умолчанию «root» (для входа в консоль управления). В целях безопасности настоятельно рекомендуется изменить этот пароль. См. *Руководство по установке SafeSpace* о других возможностях по обеспечению безопасности учетной записи root. ■

perimetrix © 2021 Perimetrix LLC

Российский разработчик программного обеспечения, основанный в 2000 г. Продуктам Perimetrix доверяют защиту конфиденциальных данных АвтоВАЗ, Газпром Энергохолдинг, Совет Федерации Федерального Собрания Российской Федерации, ТВЭЛ и другие. Компания имеет сеть партнеров в России и за рубежом. Головной офис расположен в г. Москве.

© COPYRIGHT. ALL RIGHTS RESERVED

ALL RIGHTS RESERVED. NO PART OF THIS PUBLICATION MAY BE REPRODUCED, DISTRIBUTED, OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, INCLUDING PHOTOCOPYING, RECORDING, OR OTHER ELECTRONIC OR MECHANICAL METHODS, WITHOUT THE PRIOR WRITTEN PERMISSION OF THE PUBLISHER, EXCEPT IN THE CASE OF BRIEF QUOTATIONS EMBODIED IN CRITICAL REVIEWS AND CERTAIN OTHER NONCOMMERCIAL USES PERMITTED BY COPYRIGHT LAW.